

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

POUR OBTENIR

LE TITRE DE DOCTEUR DE L'UNIVERSITÉ

PAR

Midhat GAZALÉ

- 1^{re} THÈSE. — STRUCTURES DE COMMUTATION A m VALEURS ET CALCULATRICES
NUMÉRIQUES.
- 2^e THÈSE. — PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Soutenues le 19 mai 1959 devant la Commission d'Examen.

MM. DESTOUCHES *Président.*

VILLE
DAUDEL } *Examineurs.*

PARIS

GAUTHIER-VILLARS, ÉDITEUR-IMPRIMEUR-LIBRAIRE

Quai des Grands-Augustins, 55

1959

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

POUR OBTENIR

LE TITRE DE DOCTEUR DE L'UNIVERSITÉ

PAR

Midhat GAZALÉ

1^{re} THÈSE. — STRUCTURES DE COMMUTATION A m VALEURS ET CALCULATRICES
NUMÉRIQUES.

2^e THÈSE. — PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Soutenues le 19 mai 1959 devant la Commission d'Examen.

MM. DESTOUCHES *Président.*

VILLE }
DAUDEL } *Examineurs.*

PARIS

GAUTHIER-VILLARS, ÉDITEUR-IMPRIMEUR-LIBRAIRE

Quai des Grands-Augustins, 55

1959





Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548806_0013

A MON PÈRE A MA MÈRE

A MA FEMME

A MES MAITRES ET COLLÈGUES,
grâce aux enseignements et aux encouragements desquels
cet ouvrage a pu être écrit.

INTRODUCTION

Une calculatrice dite digitale, ou numérique, a ceci de commun avec une calculatrice analogique, que sa matière d'oeuvre est l'information.

Dans l'une comme dans l'autre, on associe aux nombres des grandeurs physiques, et l'on fait correspondre aux opérations sur ces nombres des opérations sur ces grandeurs.

Dans la machine analogique, chaque nombre est représenté par une grandeur physique dont la valeur, mesurée sur une échelle appropriée, est égale au nombre en question, tandis que dans la machine digitale, chaque nombre est représenté par un ensemble fini de grandeurs physiques dont les valeurs appartiennent à un ensemble fini d'éléments discrets.

L'ensemble des valeurs associées à un nombre peut être une séquence temporelle de valeurs d'une même grandeur, ou une "configuration" spatiale des valeurs d'un ensemble de grandeurs de même nature, ou de natures différentes, ou encore une séquence de configurations.

Les organes internes de la machine digitale, servant de support à ces grandeurs physiques, sont reliés entre eux selon des lois bien précises, et l'on convient d'appeler aujourd'hui cet agencement "structure logique" de la machine à calculer.

Parmi les structures logiques, nous nous cantonnerons dans le domaine de celles qui ne font pas intervenir le temps. En effet, une machine à calculer, dans le cas le plus général, peut avoir pour modèle la célèbre machine à ruban de Turing [24], et relève de la théorie générale des structures séquentielles. Dans la présente étude, nous n'en abordons qu'un cas particulier, celui des structures dites combinatoires, ou encore "sans mémoire".

Cette distinction sera établie par la suite de façon plus précise.

Si l'on considère les machines à calculer digitales du type électronique construites à ce jour, une observation essentielle que l'on puisse faire est que la très grande majorité de celles-ci utilisent un "langage" comprenant deux symboles et deux seulement, que l'on désigne souvent par le zéro et l'unité. Ces machines sont dites binaires, et l'ensemble des

valeurs associées aux grandeurs physiques, servant de support à l'information, comprend ces deux seules valeurs.

Cet état de choses est lié de façon certaine à la stabilité de systèmes physiques utilisés à ce jour. La nature des éléments utilisés (leur non-linéarité) est telle que dans la majorité des cas, il est facile de concevoir des systèmes à deux états de stabilité, avec une marge de sécurité de fonctionnement suffisante. Il est beaucoup plus difficile, par contre, avec ces mêmes éléments, de réaliser des ensembles à plus de deux états stables. A cette limitation viennent s'ajouter d'autres considérations telles que la très grande sécurité de fonctionnement, et simplicité de conception, d'un système où un courant passe ou ne passe pas, d'une carte perforée ou non, d'un ruban magnétique aimanté par tout ou rien, etc. La loi du milieu exclu garantit donc un fonctionnement sûr et sans équivoque.

La grande majorité des calculatrices électroniques sont donc binaires et cette limitation est d'origine technologique. Théoriquement, le système de numération binaire n'est pas plus économique qu'un système ternaire (il l'est même moins) (23).

Théoriquement aussi, il n'y a aucune raison, a priori, pour que l'on ne puisse un jour inventer des systèmes multi-stables et des éléments non linéaires originaux susceptibles de donner naissance à des structures nouvelles, ternaires, par exemple.

Aujourd'hui, donc, comme l'avaient préconisé MM. R. Valtat et Couffignal en 1936 et 1938, les machines à calculer digitales universelles sont binaires.

A la même époque, Nakazima et Hanzawa, en 1936, au Japon, et C. Shannon, en 1938, aux Etats-Unis, proposèrent un rapprochement très séduisant entre la nature binaire des circuits à relais, et la logique. En effet, un contact est ouvert ou fermé et une proposition logique est vraie ou fausse. La mise en parallèle de deux contacts résulte en un circuit fermé si l'un ou l'autre des contacts est fermé (Alternation), et la mise en série de deux contacts en un circuit fermé si et seulement si les deux contacts sont fermés (Conjonction)... La logique symbolique trouvait ainsi dans le domaine des machines à calculer une application extrêmement intéressante et l'algèbre de Boole est aujourd'hui un outil dont on se sert fréquemment lors de la conception d'une machine binaire.

Il nous a semblé utile, à l'heure actuelle, d'orienter notre travail dans le sens d'une étude plus générale des structures algébriques susceptibles de trouver une application dans le domaine de la machine à calculer.

S'il s'agit de machines binaires, il est intéressant de noter que la technique actuelle donne naissance à un très grand nombre de circuits dits élémentaires, réalisant des fonctions très diverses qui ne peuvent être exploités de façon rentable que si l'ingénieur dispose de l'outil mathématique adéquat. A ces éléments nouveaux, correspondent des structures algébriques originales que l'on est aussitôt tenté d'étudier de façon plus générale.

S'il s'agit de machines ternaires, ou en général m-aires, la situation est quelque peu différente puisque la technique n'a jusqu'ici donné naissance qu'à une très petite variété de circuits susceptibles d'application. Ici l'étude est donc presque strictement théorique.

Le présent travail se situe à mi-chemin entre la technologie et la théorie dans ce sens que, guidé par les réalisations actuelles et potentielles de la première, il entreprend de suggérer une orientation et un domaine d'application à la seconde.

CHAPITRE I

DÉFINITIONS

ÉLÉMENT COMBINATOIRE

Soit un ensemble O d'objets, comprenant les trois sous-ensembles suivants :

- 1) L'ensemble des objets dits organes d'entrée ;
- 2) L'ensemble des objets dits organes de transfert ;
- 3) L'ensemble des objets dits organes de sortie .

Un élément combinatoire est un assemblage d'objets appartenant à O , ayant les propriétés suivantes :

Cet assemblage possède k organes d'entrée $e_0, e_1, e_2 \dots e_{k-1}$, un organe de sortie s et un certain nombre d'organes de transfert .

A chaque organe d'entrée ou de sortie est associée une grandeur physique mesurable, d'une nature bien déterminée (tension, courant, déplacement, vitesse, couple, etc.), dite "signal", ou "variable" d'entrée ou de sortie .

A chaque organe d'entrée e_i est associé un ensemble fini ordonné V_i de "valeurs" du signal correspondant .

A l'organe de sortie est associé un ensemble fini ordonné S de "valeurs" du signal de sortie .

A un instant donné correspond une valeur v_i , $v_i \in V_i$ pour chaque organe d'entrée e_i , et une seule .

De même, à un instant donné correspond une valeur de S et une seule .

(A deux instants distincts peuvent correspondre deux valeurs distinctes de V_i , associées à un même organe d'entrée. De même pour S .)

L'ensemble ordonné de valeurs $\langle v_0, v_1 \dots v_i \dots v_{k-1} \rangle_t$, $v_i \in V_i$, correspondant à l'instant t , est le "vecteur d'entrée", ou "configuration d'entrée", à l'instant t .

A chaque vecteur d'entrée, à un instant t donné, correspond une valeur et une seule du signal de sortie .

$$\langle v_0, v_1, \dots, v_i \dots v_{k-1} \rangle_t \longrightarrow (\sigma)_t \quad \sigma \in S \quad (1)$$

L'application ci-dessus est indépendante de l'instant considéré. Dans ce qui suit, nous supprimerons l'indice t pour simplifier l'écriture.

Cette application correspond à la réalité physique suivante :

Si l'on considère que l'élément en question fait partie d'un système physique plus étendu, comprenant un opérateur extérieur à cet élément, capable de sélectionner au hasard un vecteur de l'ensemble des vecteurs d'entrée, et s'il imprime ce vecteur à l'entrée de l'élément (ensemble ordonné des organes d'entrée), le signal de sortie "se fixera instantanément" à la valeur correspondante, par l'intermédiaire des organes de transfert.

COMBINATEUR

Dans la suite de la présente étude nous ne considérerons que des ensembles ordonnés $V_0, V_1, \dots$ et S , comprenant un même nombre m de valeurs.

Soit E l'ensemble des entiers $(0, 1, 2, \dots, m-1)$. Faisons correspondre chacun des ensembles ci-dessus à l'ensemble E ,

$$\text{l'isomorphisme} \quad E \rightleftharpoons V_i \quad (2)$$

respectant l'ordre de V_i pour chaque i .

L'application (1) peut alors s'écrire :

$$E^k \longrightarrow E \quad (3)$$

L'élément combinatoire est dit dans ce cas "combinateur" ou commutateur, E est l'ensemble des "valeurs de commutation". (3) est la "fonction de transfert" du combinateur.

On dit que le combinateur "réalise" la fonction de transfert.

STRUCTURE DE COMMUTATION

Du fait que l'ensemble E est fermé par rapport à la fonction réalisée par un combinateur, on peut concevoir des assemblages dans lesquels la sortie d'un combinateur est identifiée à une entrée appartenant à un autre combinateur.

De même, du fait que les fonctions de transfert de tous les combinateurs sont définies dans le même ensemble E , on peut concevoir des assemblages dans lesquels on identifie des entrées appartenant à deux combinateurs distincts (ou deux entrées distinctes d'un même combinateur).

Si w_1 et w_2 sont deux organes (d'entrée ou de sortie, d'un même combinateur ou de deux combinateurs distincts), on dit que l'on "connecte" w_1 à w_2 si l'on identifie à tout instant les valeurs des variables associées à w_1 et w_2 .

Nous définissons maintenant la notion de "structure combinatoire" ou simplement structure, de la manière suivante, par récurrence :

DÉFINITION a)

Un combinateur est une structure.

DÉFINITION b)

L'ensemble de deux structures, C_1 et C_2 , sans connexion aucune, est une structure C .

Toute sortie de C_1 ou de C_2 est une sortie de C .

Toute entrée de C_1 ou de C_2 est une entrée de C .

C_1 et C_2 sont des sous-structures de C .

DÉFINITION c)

L'assemblage résultant de la connexion de deux entrées quelconques d'une même structure C est une structure C' .

C est une sous-structure de C' .

Il en découle que l'assemblage résultant de la connexion de deux entrées appartenant à des structures différentes C_1 et C_2 est aussi une structure C . En effet, on peut imaginer qu'avant d'établir la connexion, on compose les deux structures distinctes, selon (b) en une structure unique.

C_1 et C_2 sont des sous-structures de C .

Si dans une structure une sortie est identique à une entrée, nous admettons par définition l'équivalence de cet assemblage à un assemblage hypothétique qui comprendrait un combinateur à une seule entrée, et dont la sortie serait identique à l'entrée.

DÉFINITION d)

L'assemblage résultant de la connexion d'une sortie quelconque d'une structure C_1 à une entrée quelconque d'une structure C_2 est une structure C . C_1 et C_2 sont des sous-structures de C .

Toute entrée de C_1 est une entrée de C .

Toute entrée de C_2 , à l'exception de celle connectée à la sortie de C_1 , est une entrée de C .

Toute sortie de C_1 ou de C_2 est une sortie de C .

Parmi les sorties de C , on distingue deux classes :

- Les sorties libres, sorties de C qui ne sont connectées à l'entrée d'aucune sous-structure de C .

- Les "connexions internes", sorties de C qui ne sont pas libres. Lorsque la même sortie d'une structure C_1 est connectée aux entrées de deux structures C_2 et C_3 , cette sortie constitue une connexion interne unique.

Une structure peut donc avoir plusieurs sorties (connexions internes et sorties libres), et plusieurs entrées.

Une structure à une seule sortie est un combinateur.

Sur l'ensemble W des organes d'entrée et de sortie d'une structure C , nous définissons la relation binaire "antérieur à", vérifiant la propriété de transitivité.

Pour $w \in W$ et $w' \in W$, w antérieur à w' s'écrit :

$$w \Rightarrow w'$$

Et l'on a, pour tout w , w' et $w'' \in W$

$$w \Rightarrow w' \quad \text{et} \quad w' \Rightarrow w'' \quad \text{entraîne} \quad w \Rightarrow w'' \dots \quad (4)$$

Si w' est la sortie d'un combinateur dont w est une entrée, nous posons par définition $w \Rightarrow w'$.

Il en découle immédiatement que deux organes quelconques w et w' de l'ensemble W satisfont la relation $\Rightarrow$

1. si w' est la sortie d'un combinateur dont w est une entrée,

2. ou s'il existe dans W un nombre fini de connexions internes $\gamma_1, \gamma_2, \dots, \gamma_n$ telles que γ_1 est la sortie d'un combinateur dont w est une entrée, γ_2 est la sortie d'un combinateur dont γ_1 est une entrée, etc., et finalement w' est la sortie d'un combinateur dont γ_n est une entrée.

Nous poserons par définition que la relation

$$w \Rightarrow w'$$

n'est vérifiée que dans le cas où l'une des conditions ci-dessus est satisfaite.

DEFINITION e)

Un assemblage n'est une structure que s'il n'existe aucun organe antérieur à lui-même.

Cette restriction ne porte en fait que sur les connexions internes. En effet, les sorties libres et les entrées satisfont cette restriction par définition, puisqu'il ne peut exister dans W aucun organe qui soit antérieur à une entrée, et il ne peut pas exister non plus d'organe auquel une sortie libre soit antérieure.

Un assemblage n'est donc une structure que s'il n'existe aucune connexion interne antérieure à elle-même.

Il en découle que dans l'ensemble W , il n'existe aucune paire de connexions internes γ et γ' telles que

$$\gamma \Rightarrow \gamma' \text{ et } \gamma' \Rightarrow \gamma$$

En effet, si cela se vérifiait, on aurait $\gamma \Rightarrow \gamma$ et $\gamma' \Rightarrow \gamma'$, ce qui est contraire à la définition e).

DÉFINITION f)

Un assemblage n'est une structure que s'il satisfait la restriction e et l'une au moins des définitions a, b, c et d.

Notons quelques conséquences intéressantes des définitions ci-dessus :

Toute structure peut par définition se décomposer en un assemblage de combinateurs, selon les règles de construction ci-dessus. Pour le moment, nous ne nous préoccupons pas de la fonction de transfert des combinateurs intervenant dans cette décomposition. Nous retenons simplement qu'à partir d'une collection de combinateurs, on peut assembler un certain nombre de structures, selon des règles précises. Nous introduirons, par la suite, la notion d'équivalence des structures, qui tiendra compte, à ce moment, de la fonction proprement dite de la structure. Nous verrons alors qu'une structure peut se décomposer en un grand nombre d'assemblages différents de combinateurs de même fonction de transfert ou de fonctions de transfert différentes.

Dans une structure donnée C, il y a autant de sorties que de combinateurs.

En effet :

a) A toute sortie de C correspond un et un seul combinateur puisqu'il n'y a pas de sortie de C qui ne soit celle d'un combinateur dans C et que l'on ne peut jamais connecter les sorties de deux combinateurs.

b) A tout combinateur correspond une et une seule sortie, par définition.

Dans une structure C à une seule sortie libre s, tous les organes de C autres que la sortie s sont antérieurs à celle-ci. Ceci se démontre simplement par récurrence sur le nombre de connexions internes de C.

Toute structure a au moins une entrée et une sortie libre. Cette proposition peut se démontrer aussi par récurrence.

Pour conclure ce chapitre, il nous semble utile de préciser que les structures combinatoires ne constituent qu'un cas particulier des structures réelles intervenant dans la construction d'une machine à calculer digitale.

En effet, afin de rendre nos définitions tout à fait générales, il nous faut introduire un élément particulier appelé retard.

Un retard est un élément à une seule entrée et une seule sortie, dont la valeur de la sortie à un instant donné t est identique à la valeur de l'entrée à l'instant $t - \Delta t$, Δt étant un temps fini, bien déterminé.

Une structure généralisée, dite "séquentielle" (1) comprendra nécessairement soit des structures combinatoires connectées entre elles par des retards, soit des structures combinatoires refermées sur elles-mêmes, ou "bouclées" à travers des retards. La restriction e est donc levée, à condition de bien spécifier que dans une structure séquentielle une sous-structure ne peut être bouclée qu'à travers un retard, et que toute sous-structure combinatoire d'une structure séquentielle satisfait (2).

La différence essentielle entre le "comportement" d'une structure séquentielle et celui d'une structure combinatoire est que dans cette dernière, à un instant donné, toutes les sorties sont déterminées par les entrées à ce même instant, indépendamment des configurations ayant précédé dans le temps, tandis que dans une structure séquentielle les sorties à un instant donné dépendent à la fois des entrées présentes et passées, la dépendance du passé étant une fonction, entre autres facteurs, du nombre de retards incorporés dans la structure, ou pour employer un langage aujourd'hui très courant, de la "mémoire" de la structure.

Une structure combinatoire est donc sans mémoire. Elle a au moins une sortie et une entrée.

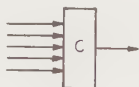
Notons pour finir qu'il existe des structures séquentielles sans entrée. Ces structures, entièrement bouclées, ne comprennent que des sorties, et pourraient être appelées "générateurs" (exemple le "multivibrateur libre").

La présente étude ne portant que sur les structures combinatoires nous n'en dirons pas plus des structures séquentielles.

Dans tout ce qui suit, "structure" sous-entendra "combinatoire".

EXEMPLES :

Dans les schémas qui suivent, un combinateur sera représenté par un rectangle associé à un certain nombre de flèches. Les flèches aboutissant au rectangle représentent les entrées, et la flèche partant du rectangle représente la sortie (fig. 1).



Exemples de structures combinatoires :

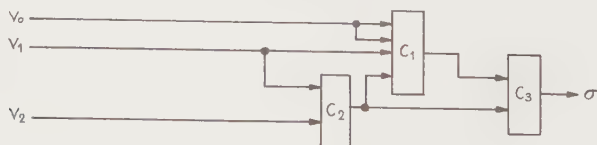


Fig. 2 (a)

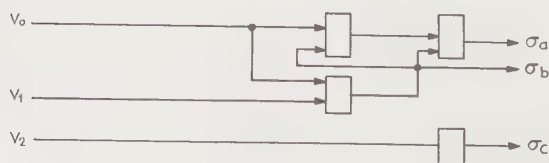


Fig. 2 (b)

CHAPITRE II

FONCTION DE TRANSFERT

Soit une structure C à plusieurs sorties libres.

A chaque sortie libre de C correspondent un certain nombre de connexions internes et d'entrées qui lui sont antérieures. La sous-structure de C dont l'ensemble des organes d'entrée et de sortie, à l'exception d'une sortie s , coïncide avec l'ensemble de tous les organes antérieurs à s est dite "aboutissant en s ".

Il est clair que, si s et s' sont deux sorties libres d'une même structure, les sous-structures y aboutissant peuvent avoir des organes en commun. Dans la pratique, le constructeur s'efforce d'ailleurs de réaliser des structures où cette coïncidence se recherche systématiquement car elle constitue un moyen d'économie appréciable.

Dans ce qui suit, il ne sera question que de structures à sortie libre unique s , ou structures aboutissant en s .

CARACTÉRISATION ARITHMÉTIQUE DES FONCTIONS DE TRANSFERT

Nous avons défini, dans le premier chapitre, la fonction de transfert d'un combinateur.

Il est facile de montrer que dans une structure aboutissant en s , ayant n entrées $e_0, e_1, \dots, e_{n-1}$, à chaque configuration des variables d'entrée $\langle v_0, v_1, \dots, v_{n-1} \rangle$, correspond une valeur et une seule de la variable de sortie σ associée à s .

σ est donc une fonction des variables d'entrée, et l'application

$$E^n \longrightarrow E$$

définit la fonction de transfert de la structure.

Le tableau de correspondance de la sortie σ aux configurations d'entrée est dit "tableau de vérité", terme que nous empruntons à la Logique.

EXEMPLES :

1°) La structure à deux entrées définie dans $E = (0, 1)$ dont la sortie prend la valeur 1 si l'une au moins des variables d'entrée prend la valeur 1, et qui autrement prend la valeur 0, a pour tableau de vérité :

v_1	v_0	σ
0	0	0
0	1	1
1	0	1
1	1	1

fig. 3

2°) La structure à deux entrées, définie dans $E = (0, 1, 2)$ dont la valeur de la sortie est égale à la somme modulo 3 des valeurs des variables d'entrée a pour tableau de vérité :

v_1	v_0	σ
0	0	0
0	1	1
0	2	2
1	0	1
1	1	2
1	2	0
2	0	2
2	1	0
2	2	1

Si, dans le tableau de la figure 3, nous associons aux configurations les nombres 0, 1, 2 et 3 dans l'ordre (de haut en bas), nous dirons que la configuration ($v_1 = 1$ et $v_0 = 0$), par exemple, a pour nombre caractéristique 2.

De façon générale, pour un m donné, soit n le nombre des variables d'entrée. Il y a donc m^n configurations d'entrée. Nous associerons à chaque configuration un nombre caractéristique selon la règle suivante :

Posons :

$$V = \sum_{i=0}^{n-1} v_i m^i \quad (5)$$

Nous dirons que la configuration d'entrée est j (ou a pour nombre caractéristique j), si et seulement si

$$V = j$$

avec j entier $0 \leq j \leq m^n - 1$ (6)

En d'autres termes, si j est un entier dont les chiffres, dans un système de numération de base m sont $\alpha_0^j, \alpha_1^j, \alpha_2^j, \dots$, c'est-à-dire

$$j = \sum_{i=0}^{n-1} \alpha_i^j \cdot m^i \quad \text{avec} \quad 0 \leq \alpha_i^j \leq m-1 \quad (7)$$

la configuration d'entrée est j si et seulement si

$$v_i = \alpha_i^j \quad (8)$$

pour toutes les valeurs de i , de 0 à $n-1$.

A chaque j correspond donc une valeur de la fonction σ . Soit σ_j cette valeur. La fonction peut donc être entièrement définie par le tableau donnant la correspondance

$$j \rightarrow \sigma_j \quad (9)$$

Une représentation équivalente consiste à partitionner l'ensemble des nombres de 0 à m^n-1 en m classes $J_0, J_1, J_\ell, \dots, J_{m-1}$, les nombres d'une même classe J_ℓ étant les valeurs de j auxquelles correspond la valeur ℓ de σ_j

L'exemple 1 ci-dessus donne dans ce cas

$$J_0 = (0)$$

$$J_1 = (1, 2, 3)$$

et l'exemple 2

$$J_0 = (0, 5, 7)$$

$$J_1 = (1, 3, 8)$$

$$J_2 = (2, 4, 6)$$

Il est quelquefois commode d'associer à une fonction un nombre caractéristique, selon la règle suivante :

On dira qu'une fonction de n variables à m valeurs a pour nombre caractéristique K , avec K entier

$$0 \leq K < m^n \quad (10)$$

si et seulement si

$$\sum_{j=0}^{m^n-1} \sigma_j \cdot m^j = K \quad (11)$$

Nous dirons de deux structures qu'elles sont équivalentes si et seulement si elles ont même nombre caractéristique K .

ANALYSE ET SYNTHÈSE DES STRUCTURES COMBINATOIRES

Etant donné une structure C aboutissant en s , on entend par analyse de la structure l'établissement du tableau de vérité de celle-ci ou de toute représentation caractérisant la fonction de transfert réalisée par elle.

Le problème inverse, appelé synthèse, consiste, à partir d'une collection de combinateurs de fonctions de transfert connues, à assembler une structure réalisant une fonction de transfert donnée.

Un combinateur réalise une fonction définie dans l'ensemble

$$E = \{0, 1, 2 \dots m-1\}$$

L'assemblage de combinateurs sous forme de structure, selon les règles définies plus haut, correspond à une composition algébrique des diverses fonctions définies dans cet ensemble.

A chaque collection de combinateurs correspond par conséquent une structure algébrique particulière avec des lois de composition précises.

Dans une structure algébrique, on suppose qu'il n'y a pas de limite au nombre de fois que l'on peut composer des variables selon une fonction donnée.

De même chaque fois que nous parlerons d'un combinateur d'une espèce donnée (d'une fonction de transfert donnée), nous supposons que le constructeur dispose d'une collection illimitée de combinateurs de cette espèce.

Le nombre de combinateurs intervenant dans une structure est donc sans importance, et seule compte la fonction qu'il réalise.

ENSEMBLES COMPLETS OU FONCTIONNELS

Nous dirons qu'un ensemble de combinateurs à m valeurs (d'espèces différentes) est "fonctionnellement complet" [2], ou fonctionnel, ou "complet" si et seulement si à partir des seuls combinateurs de cet ensemble, on peut assembler des structures réalisant toutes les fonctions de transfert définissables dans l'ensemble $E = \{0, 1, \dots, m-1\}$ (pour un nombre quelconque de variables d'entrée).

De même nous dirons d'une structure algébrique (ensemble E et les fonctions y définies) qu'elle est complète ou fonctionnelle si et seulement si les combinateurs réalisant ces fonctions constituent un ensemble complet.

EXEMPLES :

1°) G. Boole [3] a démontré que l'ensemble des fonctions suivantes définies dans l'ensemble $E = \{0, 1\}$ est fonctionnel :

v	σ
0	1
1	0

(a)

v_1	v_0	σ
0	0	0
0	1	1
1	0	1
1	1	1

fig. 5

(b)

La fonction dont le tableau de vérité est donné en 5a est dite négation, ou dans d'autres langages inversion, ou complémentation.

Celle dont le tableau est donné en 5 b est dite alternation, ou disjonction, ou opération OU inclusif, et quelquefois encore union, ce terme étant emprunté à la théorie des ensembles.

2°) E. Post [4] a démontré que l'ensemble des fonctions suivantes définies dans l'ensemble $E = (0, 1, \dots, m-1)$ est fonctionnel :

v	σ
0	m-1
1	0
2	1
3	2
.	.
.	.
.	.
m-1	m-2

(a)

v_1	v_0	σ
0	0	0
.	.	.
.	.	.
i_1	j_1	i_1 pour $i_1 \leq j_1$
.	.	.
i_2	j_2	j_2 pour $i_2 \geq j_2$
.	.	.
m-1	m-1	m-1

(b)

fig. 6

La fonction 6a est dite "cyclage de Post" et la fonction 6b "Minimum".

3°) Sheffer [5] a démontré que l'opération suivante, définie dans l'ensemble $E = (0, 1)$ est fonctionnelle (est l'élément unique d'un ensemble fonctionnel).

v_1	v_0	σ
0	0	1
0	1	1
1	0	1
1	1	0

fig. 7

ENSEMBLE SEMI-FONCTIONNEL

Une "fonction constante" ou "constante" est une fonction dont la valeur σ_j est la même pour toutes les valeurs de j (quel que soit le nombre des variables d'entrée).

Dans un ensemble $E = (0, 1, \dots, m-1)$, nous pouvons donc définir m constantes, que nous dénoterons par leurs valeurs, c'est-à-dire par $0, 1, 2 \dots m-1$.

Un ensemble de fonctions est dit "semi-fonctionnel" si l'ensemble constitué par cet ensemble et l'ensemble de toutes les constantes est fonctionnel (on considère que l'ensemble semi-fonctionnel ne comprend pas de constantes).

Notons au passage que dans la pratique, du point de vue constructeur d'une machine digitale, les ensembles semi-fonctionnels ne sont pas moins intéressants que les ensembles fonctionnels, puisqu'il dispose toujours de "sources" de signal constant.

Nous introduisons par conséquent un élément nouveau, toujours assimilable à une structure, que nous appellerons "source", et que nous représenterons schématiquement comme sur la figure 8,



fig. 8

le nombre inscrit dans le cercle représentant la valeur de la constante.

EXEMPLE :

Nous montrerons par la suite que l'ensemble des opérations somme et produit modulo p définies dans l'ensemble $E = (0, 1, \dots, p-1)$ avec p premier, est semi-fonctionnel.

Notons pour finir qu'un ensemble fonctionnel de combinateurs est dit "Redondant" s'il existe au moins un sous-ensemble véritable de cet ensemble qui soit fonctionnel.

Un ensemble fonctionnel qui n'est pas redondant est dit "irredondant".

CHAPITRE III

RAPPEL DE QUELQUES RÉSULTATS CONCERNANT LES ENSEMBLES FONCTIONNELS

1°) Comme nous l'avons indiqué plus haut, G. Boole a démontré que l'ensemble des fonctions "OU" et "inversion" est fonctionnel, dans l'ensemble $E = (0, 1)$.

De même l'ensemble des fonctions "inversion" et "ET", (défini par le tableau de la figure 9), est fonctionnel.

v_1	v_0	σ
0	0	0
0	1	0
1	0	0
1	1	1

fig. 9

L'ensemble des fonctions "ET", "OU" et "inversion" est par conséquent un ensemble fonctionnel redondant.

Il est utile de préciser le rôle considérable que cette structure algébrique, dite algèbre de Boole, a joué, jusqu'aujourd'hui, dans la conception des ensembles logiques des calculatrices digitales. En effet, comme l'ont montré d'une part Nakazima et Hanzawa (8), au Japon, en 1936, et d'autre part C. Shannon (9) aux Etats-Unis en 1938, les structures à relais peuvent être entièrement représentées par un modèle algébrique où la mise en série de contacts de relais correspond à une loi de composition "ET" des variables associées aux relais, la mise en parallèle à une loi de composition "OU" de ces variables, et un contact "normalement fermé" à une inversion (1).

L'apparition des lampes à vide dans le domaine de la machine à calculer a apporté une complication à cette situation, puisque les fonctions élémentaires réalisables par les combineteurs nouveaux n'étaient plus de simples "OU" et "ET". Quelques années plus tard, l'utilisation systématique des diodes au germanium rétablissait la situation antérieure, puisqu'on pouvait de nouveau réaliser à peu de frais des circuits ET et des circuits OU.

(1) Gavrilov, en U.R.S.S., aurait établi cette même corrélation, à cette époque.

Aujourd'hui, avec l'introduction du transistor, la situation se complique à nouveau, puisque, dans les machines actuelles, les "unités connectables" ont des fonctions de transfert compliquées. Il est donc utile d'aborder des structures algébriques nouvelles mieux adaptées aux besoins créés par les combinateurs actuels.

2°) Dans l'ensemble $E = (0, 1, \dots, m-1)$, l'ensemble des fonctions cyclage et minimum de Post est fonctionnel.

Une troisième fonction, le "Maximum" (fig. 11) constitue avec les deux premières une structure redondante connue sous le nom d'Algèbre de Post, qui est une généralisation de l'Algèbre de Boole pour $m \geq 2$.

v_1	v_0	σ	
0	0	0	
.....			
.....			
i_1	j_1	i_1 pour $i_1 \geq j_1$	fig. 11
i_2	j_2	j_2 pour $i_2 \leq j_2$	
.....			
m-1	m-1	m-1	

3°) Nous avons indiqué plus haut que la fonction de Sheffer est fonctionnelle. Une autre fonction, apparentée à celle-ci, et quelquefois appelée fonction de Peirce, est aussi fonctionnelle dans l'ensemble $E = (0, 1)$.

v_1	v_0	σ	
0	0	1	
0	1	0	fig. 10
0	0	0	
1	1	0	

Il a d'ailleurs été démontré que la fonction de Sheffer et la fonction de Peirce sont les deux seules opérations (fonctions de deux arguments) fonctionnelles, qu'il soit possible de définir dans l'ensemble $E = (0, 1)$. Voir à ce sujet H. Freudenthal [10] et Zylinski [11].

3°) S. Piccard [12] a démontré que les fonctions suivantes, définies dans un ensemble $E = (0, 1 \dots m-1)$ constituent un ensemble qui suffit à engendrer toutes les fonctions d'une seule variable.

- a) $f(0) = m-1$
 $f(i) = i-1$ pour $1 \leq i \leq m-1$
- b) $g(m-2) = m-1$
 $g(m-1) = m-2$
 $g(i) = i$ pour $0 \leq i \leq m-3$
- c) $h(0) = 1$
 $h(i) = i$ pour $1 \leq i \leq m-1$

N.M. Martin [13] a étendu ce résultat aux fonctions plus générales définies comme suit :

Si $A_0, A_1, \dots, A_{m-1}$ est une permutation des valeurs $0, 1, \dots, m-1$,

$$\begin{aligned} \text{a) } f(A_0) &= A_{m-1} \\ f(A_i) &= A_{i-1} \quad \text{pour } 1 \leq i \leq m-1 \end{aligned}$$

b) Il existe une valeur de j telle que

$$\begin{aligned} g(A_j) &= A_{j+1 \pmod{m}} \\ g(A_{j+1 \pmod{m}}) &= A_j \\ g(i) &= i \quad \text{pour } i \neq A_j \quad \text{et} \quad i \neq A_{j+1 \pmod{m}} \end{aligned}$$

c) $h(p)$ est une fonction prenant exactement $m-1$ valeurs.

5°) Szupecki [14] a démontré que pour $m > 2$ un ensemble est fonctionnel si et seulement s'il suffit à exprimer toutes les fonctions d'une seule variable et au moins une fonction $f(p, q)$ de deux variables telle que

$$\begin{aligned} f(k, t) &\neq f(k, r) \\ f(k, t) &\neq f(s, t) \\ \text{et} \quad f(k, r) &\neq f(s, t) \end{aligned}$$

pour $0 \leq k, r, s, t, \leq m-1$.

Ce qui revient à dire que $f(p, q)$ n'est égale à aucune fonction d'une seule variable.

6°) N.M. Martin [13] a démontré que $f(p, q)$ est fonctionnelle si et seulement s'il existe une valeur de $i > 0$ telle que toutes les fonctions de i variables peuvent être exprimées à partir de $f(p, q)$ seule (par une itération finie de celle-ci).

7°) J.D. Swift [6] a isolé toutes les opérations (fonctions de deux arguments) fonctionnelles symétriques pour $m = 3$.

Ce résultat a été étendu par N.M. Martin qui a réussi à isoler toutes les opérations fonctionnelles pour $m = 3$.

8°) D.L. Webb [15] a démontré l'existence d'au moins une opération fonctionnelle pour un m quelconque.

Il a aussi démontré que la fonction suivante est fonctionnelle ; dans l'ensemble $E = (0, 1, \dots, m-1)$

$$\begin{aligned} W(i, j) &= 0 & \text{pour } i \neq j \\ \text{et } W(i, j) &= i+1 \pmod{m} & \text{pour } i = j. \end{aligned}$$

Nous conviendrons d'appeler la fonction ci-dessus fonction de Webb.

9°) C.Y. Lee et W.H. Chen (16) ont démontré que la fonction "T" définie ci-dessous est semi-fonctionnelle :

La fonction T est une fonction de $m+1$ variables

$T(v_0, v_1, \dots, v_i, \dots, v_{m-1}, \mu)$ telle que

$T(v_0, v_1, \dots, v_i, \dots, v_{m-1}, \mu) = v_i$ pour $\mu = i$ (pour toutes les valeurs de i).

10°) Łukasiewicz et Tarski (19) ont défini dans l'ensemble $E' = (1, 2, \dots, m)$ les fonctions suivantes :

$$\sim i = (m+1) - i$$

$$\text{et} \quad \begin{cases} i \rightarrow j = 1 & \text{pour } i \geq j \\ i \rightarrow j = (j-i) + 1 & \text{pour } i < j \end{cases}$$

Celles-ci ne constituent pas un ensemble fonctionnel (20). Toutefois Słupecki (21) a montré que l'adjonction de la constante 2 suffisait à le rendre fonctionnel. (L'ensemble est donc semi-fonctionnel).

Récemment, T. Evans et P.B. Schwartz (22) ont montré que 2 n'était pas la seule constante à jouir de cette propriété. En effet, l'adjonction d'une constante k rend cet ensemble fonctionnel si et seulement si $(m-1)$ est premier à $(k_0 - 1)$, avec $k_0 = \min(k, \sim k)$.

11°) Il nous semble utile de citer ici la fonction "décision majoritaire" de Von Neumann [25], fonction d'un nombre impair d'entrées, définie dans $E = \{0, 1\}$, qui prend la valeur 1 si et seulement si la majorité des entrées ont pour valeur 1.

Cette fonction, utilisée par McCulloch et Pitts en 1943 pour servir de modèle aux neurones, est aujourd'hui très abondamment utilisée par les Japonais lors de la conception des circuits utilisant le "Parametron".

CHAPITRE IV

L'ENSEMBLE SEMI-FONCTIONNEL

SOMME, PRODUIT, IDENTITÉ

Nous définissons maintenant un ensemble semi-fonctionnel comprenant trois opérations simples que nous appelons Somme généralisée, Produit généralisé, et Identité.

LA SOMME

Toute opération, définie dans l'ensemble $E = (0, 1, \dots, m-1)$, dont l'élément neutre (à droite et à gauche) est le zéro, sera dite somme, et dénotée par le symbole $+$, c'est-à-dire $a + 0 = 0 + a = a$ pour tout élément a de E .

Une somme particulière n'est évidemment définie que si sa valeur est définie pour toutes les configurations restantes, c'est-à-dire si son tableau de vérité est complété.

EXEMPLES :

a) Pour $E = (0, 1)$, chaque valeur affectée à X dans le tableau suivant

v_1	v_0	σ
0	0	0
0	1	1
1	0	1
1	1	X

fig. 12

définit une somme particulière

$X = 1$ définit la fonction "OU" ou somme logique, mentionnée plus haut,
 $X = 0$ définit la somme modulo 2.

La première sera dénotée

$$v_0 + v_1 \quad \text{log.}$$

et la seconde

$$v_0 + v_1 \quad \text{mod } 2.$$

Les deux sommes ainsi définies sont commutatives et associatives. Seule la somme mod. 2 définit une structure de groupe.

b) Pour $E = (0, 1, 2)$, on peut définir 4^3 sommes différentes en affectant aux symboles X, Y_1, Y_2 et Z dans le tableau de la figure 13 les valeurs 0, 1 et 2 de toutes les manières possibles.

	0	1	2
0	0	1	2
1	1	X	Y_1
2	2	Y_2	Z

fig. 13

Si l'on ne recherche que les sommes commutatives, on posera $Y_1 = Y_2 = Y$.

Le tableau de la figure 14 donne les 9 combinaisons de valeurs affectées à X, Y et Z telles que la somme soit aussi associative.

X	Y	Z
0	2	2
1	1	0
1	1	1
1	1	2
1	2	1
1	2	2
2	0	1
2	1	2
2	2	2

fig. 14

Parmi toutes les sommes ainsi définies, il est aisé de voir que seule la somme correspondant à $X = 2, Y = 0$ et $Z = 1$ est telle qu'à tout élément a corresponde un inverse a' (élément opposé).

$$a' + a = a + a' = 0.$$

Celle-ci n'est autre que la somme modulo 3.

En d'autres termes, la somme modulo 3 est la seule somme qui définit une structure de groupe abélien dans l'ensemble $E = (0, 1, 2)$.

LE PRODUIT

Toute opération définie dans l'ensemble $E = (0, 1, \dots, m-1)$ ayant l'unité pour élément neutre et le zéro pour élément permis sera dite "Produit" et dénotée par le signe $\times$, un point ou la juxtaposition des symboles, sans signe.

On a donc

$$0.a = a.0 = 0$$

et

$$1.a = a.1 = a.$$

EXEMPLES

a) Pour $E = (0, 1)$, on ne peut définir qu'un seul produit qui sera indifféremment appelé produit logique, produit modulo 2, etc. Celui-ci est distributif par rapport à la somme logique et à la somme modulo 2. Il définit avec la seconde une structure d'anneau commutatif.

b) Pour $E = (0, 1, 2)$, le tableau de la figure 15 indique que l'on ne peut définir que 3 produits différents, tous commutatifs.

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	U

fig. 15

Pour $U = 1$ le tableau définit le produit modulo 3.

Pour $m = 3$, il est aisé de voir que tous les produits sont associatifs.

Il est intéressant d'isoler les combinaisons de valeurs de U, X, Y et Z , pour lesquelles le produit est doublement distributif (à gauche et à droite) par rapport à la somme (celle-ci étant commutative).

Le tableau de la figure 16 donne ces combinaisons pour $m = 3$.

U	X	Y	Z
0	0	1	0
0	1	1	2
0	2	1	0
1	0	0	0
1	1	0	2
1	2	0	1
2	0	0	0
2	1	1	2
2	1	2	2
2	2	1	2
2	2	2	2

fig. 16

Si nous éliminons les combinaisons pour lesquelles la somme n'est pas associative, nous obtenons le tableau de la figure 17.

U	X	Y	Z
0	1	1	2
1	2	0	1
2	1	1	2
2	1	2	2
2	2	1	2
2	2	2	2

fig. 17

Dans ce tableau, on voit donc que la seule combinaison qui donne une structure d'anneau commutatif est la suivante :

$$U = 1 \quad X = 2 \quad Y = 0 \quad Z = 1 .$$

En d'autres termes, seuls le produit modulo 3 et la somme modulo 3 donnent à l'ensemble $E = (0, 1, 2)$ une structure d'anneau commutatif.

FONCTION IDENTITÉ

Nous appelons fonction caractéristique de la matrice identité, ou plus simplement fonction Identité, ou encore fonction Kronecker, la fonction définie comme suit :

$$\begin{array}{ll} I(a, b) = \tilde{0} & \text{pour } a \neq b \\ \text{et} & I(a, b) = 1 \quad \text{pour } a = b \\ \text{avec} & a, b \in E. \end{array}$$

Propriétés remarquables de la Somme

Soit A un ensemble $(a_0, a_1, \dots, a_k)$ d'éléments de E , tel qu'il existe au plus une valeur de i pour laquelle $a_i \neq 0$.

On vérifie que la Somme est commutative dans l'ensemble A , et que celui-ci est fermé par rapport à celle-là. De même, la somme est associative dans l'ensemble A . Nous conviendrons d'écrire la somme $a_0 + a_1 + \dots + a_k$ sous la forme

$$\sum_{i=0}^k a_i$$

Propriétés remarquables du Produit

Soit A' un ensemble $(a_0, a_1, \dots, a_k)$ d'éléments appartenant au sous ensemble $(0, 1)$ de E . On vérifie que le Produit est commutatif dans l'ensemble A' , et que celui-ci est fermé par rapport à celui-là. De même, le Produit est associatif dans l'ensemble A' . Nous conviendrons d'écrire le produit $a_1 \cdot a_2 \cdot \dots \cdot a_k$ sous la forme

$$\prod_{i=0}^k a_i$$

THÉORÈME 1

L'ensemble d'une somme quelconque, d'un produit quelconque et d'une fonction identité est semi-fonctionnel.

En effet, soit à exprimer une fonction σ , de n variables. Soit σ_j , la valeur de σ correspondant à la configuration j . Considérons la fonction Identité

$$I(\alpha_i^j, v_i) \quad (12)$$

α_i^j étant une constante égale au $i^{\text{ème}}$ chiffre de j dans un système de numération de base m .

$$\begin{aligned} \text{On a :} \quad I(\alpha_i^j, v_i) &= 1 \quad \text{pour} \quad \alpha_i^j = v_i \\ &= 0 \quad \text{pour} \quad \alpha_i^j \neq v_i \end{aligned} \quad (13)$$

Considérons maintenant le produit

$$\prod_{i=0}^{n-1} I(\alpha_i^j, v_i) \quad (14)$$

pour une valeur donnée de j , $\prod$ représentant un produit quelconque répété.

On a :

$$\prod_{i=0}^{n-1} I(\alpha_i^j, v_i) = 1 \text{ si et seulement si } \alpha_i^j = v_i \text{ pour toutes les valeurs de } i$$

$$\text{et} \quad = 0 \text{ dans tous les autres cas.} \quad (15)$$

Nous écrirons ce produit, pour simplifier l'écriture, sous la forme suivante :

$$\prod_{i=0}^{n-1} I(\alpha_i^j, v_i) = I(j, V) \quad (16)$$

$$\begin{aligned} \text{Et nous aurons :} \quad I(j, V) &= 1 \quad \text{pour} \quad j = V \\ &= 0 \quad \text{pour} \quad j \neq V \end{aligned} \quad (17)$$

En d'autres termes, $I(j, V)$ est une fonction des variables d'entrée $v_0, v_1 \dots v_{n-1}$ qui est égale à l'unité si et seulement si la configuration d'entrée est j , et est égale à 0 dans tous les autres cas.

Considérons maintenant le produit

$$\sigma_j \cdot I(j, V) \quad (18)$$

Le membre de droite de ce produit étant soit 0, soit 1, on a :

$$\sigma_j \cdot I(j, V) = \sigma_j \quad \text{pour} \quad j = V \quad (19)$$

$$\text{et} \quad = 0 \quad \text{pour} \quad j \neq V \quad (20)$$

quel que soit le produit choisi.

Considérons maintenant la somme

$$\sigma_0 \cdot I(0, V) + \sigma_1 \cdot I(1, V) + \dots + \sigma_j \cdot I(j, V) + \dots + \sigma_{m^n-1} \cdot I(m^n-1, V) \quad (21)$$

Dans l'expression ci-dessus, pour une valeur donnée de j , on ne peut avoir qu'un seul terme différent de 0.

L'expression (21) prend donc la même valeur quelle que soit la somme choisie. Le symbole + représente par conséquent une somme quelconque. Nous écrirons l'expression (21) sous la forme :

$$\sum_{j=0}^{m^n-1} \sigma_j \cdot I(j, V) \quad (22)$$

le symbole $\sum$ représentant une somme quelconque,
et l'on a :

$$\sum_{j=0}^{m^n-1} \sigma_j \cdot I(j, V) = \sigma_j \quad \text{si et seulement si } j = V, \\ \text{pour toutes les valeurs de } j.$$

On a donc :

$$\sigma(v_0, v_1, \dots, v_{n-1}) = \sum_{j=0}^{m^n-1} \sigma_j \cdot I(j, V) \quad (23)$$

$$= \sum_{j=0}^{m^n-1} \left[\sigma_j \cdot \prod_{i=0}^{n-1} I(\alpha_i^j, v_i) \right] \quad (24)$$

L'expression (24) représente la fonction σ , quelles que soient la somme et le produit utilisés.

Dans cette expression n'apparaissent que les variables $v_0, v_1, \dots, v_{n-1}$, les constantes α et σ_j , l'Identité, la somme et le produit. L'ensemble des trois dernières fonctions est donc semi-fonctionnel. Nous appellerons cette expression Forme Canonique A.

EXEMPLES :

1°) Pour $m = 2$, la forme canonique A s'écrit :

$$\sigma = \sum_{j=0}^{2^n-1} \left[\sigma_j \prod_{i=0}^{n-1} I(\alpha_i^j, v_i) \right] \quad (25)$$

Pour $n = 1$, on a :

$$\sigma(v_0) = \sigma_0 I(0, v_0) + \sigma_1 I(1, v_1) \quad (26)$$

Pour $n = 2$,

$$\begin{aligned} \sigma(v_0, v_1) &= \sigma_0 I(0, V) + \sigma_1 I(1, V) + \sigma_2 I(2, V) + \sigma_3 I(3, V) \\ &= \sigma_0 \cdot I(0, v_0) \cdot I(0, v_1) + \sigma_1 \cdot I(1, v_0) I(0, v_1) \\ &\quad + \sigma_2 I(0, v_0) \cdot I(1, v_1) + \sigma_3 I(1, v_0) I(1, v_1) \end{aligned} \quad (27)$$

En supposant que l'on dispose de combinateurs réalisant une fonction somme, une fonction produit et une fonction identité, on peut construire

par exemple, une structure dite "universelle" à deux variables d'entrée v_0 et v_1 (fig. 18).

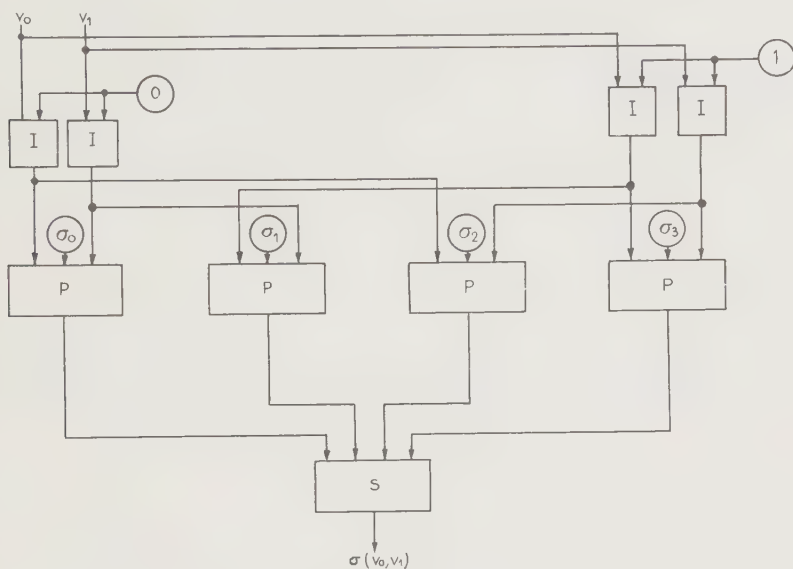
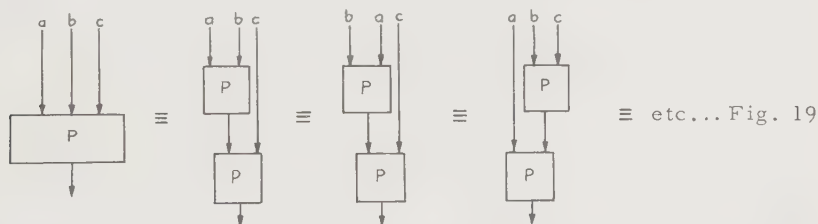


Fig. 18

Sur cette figure on a représenté des combinateurs Identité (rectangles portant un symbole I), des structures à 3 entrées et une sortie portant un symbole P et une structure à 4 entrées et une sortie portant le symbole S.

La structure P réalise le produit de trois variables d'entrées, et peut être construite de plusieurs manières à partir de combinateurs "Produit", la fonction Produit étant associative et commutative (fig. 19).



De même, la structure S réalise la somme de 4 variables d'entrée et peut être construite à partir de combinateurs "Somme" de plusieurs manières différentes

$$a + b + c + d = a + (b + c + d) = a [b + (c + d)] \quad \text{etc.}$$

Dans la structure de la figure 18, il suffit de fixer la valeur du signal de chacune des sources σ_0 , σ_1 , σ_2 et σ_3 à la valeur correspondante du tableau de vérité pour réaliser une fonction particulière donnée.

On peut vérifier aisément que si $\bar{\alpha}$ dénote la négation, ou inversion de α , l'on peut écrire

$$I(\alpha_i^j, v_i) = \alpha_i^j v_i + \bar{\alpha}_i^j \bar{v}_i \log \quad (28)$$

la somme ci-dessus étant la somme logique, ou alternation.

Ceci nous donne :

$$\sigma(v_0, v_1, \dots, v_{n-1}) = \sum_{j=0}^{2^n-1} \left[\sigma_j \prod_{i=0}^{n-1} (\alpha_i^j v_i + \bar{\alpha}_i^j \bar{v}_i) \right] \log. \quad (29)$$

Et, avec $\bar{0} = 1$ et $\bar{1} = 0$, on peut écrire, pour $n = 1$

$$\sigma(v_0) = \sigma_0 \bar{v}_0 + \sigma_1 v_0 \log. \quad (30)$$

et pour $n = 2$

$$\sigma(v_0, v_1) = \sigma_0 \bar{v}_0 \bar{v}_1 + \sigma_1 v_0 \bar{v}_1 + \sigma_2 \bar{v}_0 v_1 + \sigma_3 v_0 v_1 \quad (31)$$

De façon générale, si l'on convient que, v étant une variable quelconque,

$$v^\alpha = \bar{v} \quad \text{pour} \quad \alpha = 0$$

$$\text{et} \quad v^\alpha = v \quad \text{pour} \quad \alpha = 1$$

l'expression (29) devient :

$$\sigma(v_0, v_1, \dots, v_{n-1}) = \sum_{j=0}^{2^n-1} \left[\sigma_j \prod_{i=0}^{n-1} v_i^{\alpha_i^j} \right] \log. \quad (32)$$

L'expression ci-dessus, connue sous le nom de "forme canonique disjonctive", consiste en une somme (logique) répétée de produits (logiques) des variables et de leurs négations. Un produit de cette expression est quelquefois appelé "Minterme" ou terme minima.

La structure de la figure 18 peut être maintenant transformée en une structure équivalente en remplaçant les deux combineteurs identité de gauche par des combineteurs "inversion" et ceux de droite par une simple connexion de l'entrée à la sortie.

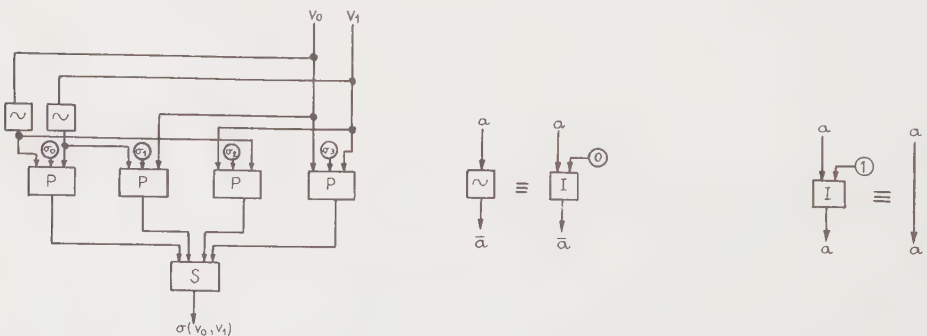


Fig. 20

2°) Toujours pour $m = 2$, on vérifie aisément ce qui suit :

$$I(a, b) = 1 + a + b \text{ modulo } 2 \quad (33)$$

pour $a, b \in E$.

La fonction identité peut donc s'exprimer à partir de la somme modulo 2. Pour $m = 2$ on en déduit que l'ensemble de la somme modulo 2 et du produit modulo 2 est semi-fonctionnel.

Pour $m = 2$, la forme canonique A devient :

$$\sigma(v_0, v_1, \dots, v_{n-1}) = \sum_{j=0}^{2^n-1} \left[\sigma_j \prod_{i=0}^{n-1} (1 + \alpha_i^j + v_i) \right] \text{ mod. } 2 \quad (34)$$

Et, en particulier, pour $n = 2$, par exemple,

$$\begin{aligned} \sigma(v_0, v_1) &= \sigma_0(1+v_0)(1+v_1) + \sigma_1 v_0(1+v_1) + \sigma_2(1+v_0)v_1 + \sigma_3 v_0 v_1 \\ &= a_0 + a_1 v_0 + a_2 v_1 + a_3 v_0 v_1 \text{ mod. } 2 \end{aligned} \quad (35)$$

avec

$$\begin{aligned} a_0 &= \sigma_0 \text{ mod. } 2 \\ a_1 &= \sigma_0 + \sigma_1 \text{ mod. } 2 \\ a_2 &= \sigma_0 + \sigma_2 \text{ mod. } 2 \\ a_3 &= \sigma_0 + \sigma_1 + \sigma_2 + \sigma_3 \text{ mod } 2 \end{aligned} \quad (36)$$

3°) Pour $m = 3$, on peut vérifier ce qui suit :

$$I(a, b) = 1 + 2a^2 + 2b^2 + 2ab \text{ mod. } 3 \quad (37)$$

pour

$$a, b \in E$$

avec

$$a^2 = a \cdot a \text{ mod. } 3$$

On en déduit alors que pour $m = 3$ l'ensemble de la somme modulo 3 et du produit modulo 3 est semi-fonctionnel, et l'on a pour $n = 1$, par exemple :

$$\sigma(v_0) = a_0 + a_1 v_0 + a_2 v_0^2 \text{ mod. } 3 \quad (38)$$

avec

$$\left. \begin{aligned} a_0 &= \sigma_0 \\ a_1 &= 2\sigma_1 + \sigma_2 \\ a_2 &= 2(\sigma_0 + \sigma_1 + \sigma_2) \end{aligned} \right\} \text{ mod. } 3$$

En s'inspirant de la manière dont la structure de la figure 18 est construite, on peut imaginer une structure universelle réalisant une fonction d'un nombre quelconque de variables.

GÉNÉRALISATION

Nous concluons ce chapitre en remarquant que la forme canonique A, définie à partir de la Somme, du Produit et de l'Identité, peut être consi-

dérée comme un cas particulier d'une forme encore plus générale, définie à partir des opérations suivantes :

Soit $e, d \in E$ $e \neq d$.

1°) L'opération J

$$\begin{aligned} J(a, b) &= e \quad \text{pour } a = b \\ J(a, b) &= d \quad \text{pour } a \neq b, \text{ pour tout } a \text{ et } b \in E. \end{aligned}$$

2°) L'opération ϕ

$$\begin{aligned} e \phi a &= a \phi e = a \quad \text{pour tout } a \in E \\ d \phi a &= a \phi d = d \quad \text{pour tout } a \in E. \end{aligned}$$

Il découle de cette définition que l'ensemble $A' = (a_0, a_1, \dots, a_k)$ d'éléments appartenant au sous ensemble (e, d) de E est fermé par rapport à l'opération ϕ . Celle-ci est commutative et associative dans l'ensemble A' .

Nous conviendrons d'écrire :

$$a_0 \phi a_1 \phi a_2 \dots \phi a_k = \bigoplus_{i=0}^k a_i.$$

3°) L'opération ψ

$$d \psi a = a \psi d = a \quad \text{pour tout } a \in E.$$

Il découle de cette définition que l'ensemble $A = (a_0, a_1, \dots, a_k)$ d'éléments de E tel qu'il existe au plus une valeur de i pour laquelle $a_i \neq d$, est fermé par rapport à l'opération ψ . Celle-ci est commutative et associative dans l'ensemble A . Nous conviendrons d'écrire :

$$a_0 \psi a_1 \psi a_2 \dots \psi a_k = \biguplus_{i=0}^k a_i.$$

Nous pouvons alors écrire

$$\sigma(v_0, v_1 \dots v_{n-1}) = \biguplus_{j=0}^{m-1} \left[\sigma_j \phi \bigoplus_{i=0}^{n-1} J(\alpha_i^j, v_i) \right] \quad (39)$$

En effet, pour $j \neq V$, il existe au moins une valeur de i pour laquelle $\alpha_i^j = v_i$, c'est-à-dire, pour laquelle $J(\alpha_i^j, v_i) = d$, et l'on a par conséquent :

$$\bigoplus_{i=0}^{n-1} J(\alpha_i^j, v_i) = d$$

$$\text{et} \quad \sigma_j \phi \bigoplus_{i=0}^{n-1} J(\alpha_i^j, v_i) = d$$

Par contre, pour $j = V$ on a $\alpha_i^j = v_i$ pour toutes les valeurs de i c'est-à-dire $J(\alpha_i^j, v_i) = e$ pour toutes les valeurs de i , et par conséquent

$$\bigoplus_{i=0}^{n-1} J(\alpha_i^j, v_i) = e$$

$$\text{et} \quad \sigma_j \phi \bigoplus_{i=0}^{n-1} J(\alpha_i^j, v_i) = \sigma_j$$

et ce, pour toute valeur de j .

Cas particulier de $m=2$

Si nous posons $e = 1$ et $d = 0$ l'opération $J(a, b)$ coïncide avec l'Identité $I(a, b)$, l'opération ϕ avec le produit et l'opération ψ avec la somme. On retrouve donc la forme canonique A.

Si nous posons $e = 0$ et $d = 1$, nous obtenons

$$\begin{aligned} 0 \phi a &= a \phi 0 = a \\ \text{et} \quad 1 \phi a &= a \phi 1 = 1 \quad \text{pour tout } a \in E \end{aligned}$$

L'opération ϕ se confond par conséquent avec la somme logique, ou alternation, ou disjonction.

De même, nous obtenons

$$1 \psi a = a \psi 1 = a.$$

Le tableau de vérité de cette opération

	0	1
0	X	0
1	0	1

peut être complété de deux manières différentes, selon la valeur de X.

1°) Soit $X = 0$

L'opération ϕ se confond avec le produit logique, ou conjonction, et l'on obtient :

$$\sigma(v_0, v_1 \dots v_{n-1}) = \prod_{j=0}^{2^n-1} \left[\sigma_j + \sum_{i=0}^{n-1} J(\alpha_i^j, v_i) \right] \log \quad (40)$$

Il est clair que $J(0, a) = I(1, a)$ et inversement, $J(1, a) = I(0, a)$. On peut donc construire une structure réalisant (40) à partir de la structure de la figure 18 en remplaçant :

- a) la source 0 par une source 1 et inversement ;
- b) chaque combinateur somme par un combinateur produit, et inversement.

En introduisant la fonction "négation" on peut alors écrire :

$$J(a, b) = a\bar{b} + \bar{a}b \quad \log.$$

Ce qui nous donne :

$$\sigma(v_0, v_1 \dots v_{n-1}) = \prod_{j=0}^{2^n-1} \left[\sigma_j + \sum_{i=0}^{n-1} (\alpha_i^j \bar{v}_i + \bar{\alpha}_i^j v_i) \right] \log \quad (41)$$

Cette forme est communément appelée forme canonique conjonctive. ou "duale" de la forme canonique disjonctive.

On a, par exemple, pour $n = 1$

$$\sigma(v_0) = (\sigma_0 + v_0)(\sigma_1 + \bar{v}_0).$$

Et pour $n = 2$:

$$\sigma(v_0, v_1) = (\sigma_0 + v_0 + v_1)(\sigma_1 + \bar{v}_0 + v_1)(\sigma_2 + v_0 + \bar{v}_1)(\sigma_3 + \bar{v}_0 + \bar{v}_1) \quad (42)$$

On peut donc construire une structure réalisant (42) à partir de celle de la figure 19 en remplaçant :

- a) chaque variable v_i par son inverse $\bar{v}_i$;
- b) chaque combinateur somme par un combinateur produit, et inversement

2°) Soit $X = 1$

L'opération ϕ se confond alors avec la fonction Identité, et nous conviendrons d'écrire (39) sous la forme :

$$\sigma(v_0, v_1 \dots v_{n-1}) = \prod_{j=0}^{2^n-1} \left[\sigma_j + \sum_{i=0}^{n-1} J(\alpha_i^j, v_i) \right] \quad (43)$$

$\prod$ dénote l'identité répétée (opération commutative et associative dans l'ensemble $(0,1)$)

+ la somme logique et $\sum$ la somme logique répétée.

En remarquant que

$$J(a, b) = I(\bar{a}, b) = I(a, \bar{b})$$

nous pouvons écrire

$$\text{soit} \quad J(\alpha_i^j, v_i) = I(\alpha_i^j, \bar{v}_i) \quad (44)$$

$$\text{soit} \quad J(\alpha_i^j, v_i) = I(\bar{\alpha}_i^j, v_i) \quad (45)$$

En substituant (45) dans (43), il vient :

$$\sigma(v_0, v_1 \dots v_{n-1}) = \prod_{j=0}^{2^n-1} \left[\sigma_j + \sum_{i=0}^{n-1} I(\bar{\alpha}_i^j, v_i) \right] \quad (46)$$

Et l'on a par exemple, pour $n = 1$

$$\sigma(v_0) = I \left\{ \left[\sigma_0 + I(1, v_0) \right], \left[\sigma_1 + I(0, v_0) \right] \right\} \quad (47)$$

d'où la structure :

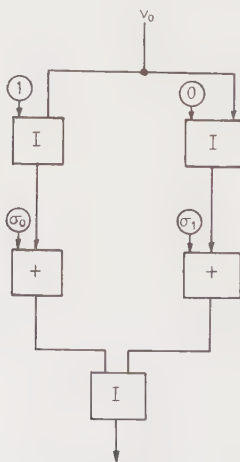


Fig. 21

et, pour $n = 2$

$$\sigma(v_0, v_1) = \prod \left\{ \left[\sigma_0 + I(1, v_0) + I(1, v_1) \right], \left[\sigma_1 + I(0, v_0) + I(1, v_1) \right], \left[\sigma_2 + I(1, v_0) + I(0, v_1) \right], \left[\sigma_3 + I(0, v_0) + I(0, v_1) \right] \right\} \quad (48)$$

On peut alors construire une structure réalisant 48 à partir de celle de la figure 18 en remplaçant

- a) La source 0 par une source 1 et inversement,
- b) Les combinateurs P par des combinateurs "Somme logique",
- c) Le combinateur S par un combinateur I.

Cet ensemble illustre le résultat suivant (contenu dans (46)) :

Dans l'ensemble $E = \{0, 1\}$ l'ensemble des opérations Identité et Somme Logique est semi-fonctionnel.

AUTRE PROPRIÉTÉ REMARQUABLE DE LA SOMME ET DU PRODUIT

Si le produit est distributif par rapport à la somme, ces deux opérations étant commutatives et associatives, on a

$$\prod_{i=0}^{n-1} \sum_{q=0}^{m-1} \phi_i(q) = \prod_{k=0}^{m-1} \sum_{i=0}^{n-1} \phi_i(\alpha_i^k) \quad (49)$$

avec

$$q \in E = \{0, 1, \dots, m-1\}$$

et

$\phi_0(q), \phi_1(q) \dots \phi_i(q) \dots$ désignant n fonctions de q prenant leurs valeurs dans E , avec n quelconque.

La relation (49) se démontre par récurrence sur n .

Pour $n = 1$ celle-ci nous donne

$$\sum_{q=0}^{m-1} \phi_0(q) = \sum_{k=0}^{m-1} \phi_0(\alpha_0^k) \quad (50)$$

en effet, dans ce cas, $k \in E$, et $\alpha_0^k = k$.

Supposons maintenant (49) vérifiée pour une valeur N de n

$$\prod_{i=0}^{N-1} \sum_{q=0}^{m-1} \phi_i(q) = \sum_{k=0}^{m-1} \prod_{i=0}^{N-1} \phi_i(\alpha_i^k) \quad (51)$$

Posons

$$K = k + m^N \xi \quad (52)$$

avec

$$\begin{aligned} 0 &\leq \xi \leq m-1 \\ 0 &\leq k \leq m^{N-1} \\ \text{et} \quad 0 &\leq K \leq m^{N+1}-1 \end{aligned}$$

et désignons par $(\phi_0, \phi_1, \dots, \phi_K, \text{ et } \phi_{m^{N+1}-1})$, p^{N+1} expressions prenant leurs valeurs dans E .

Nous pouvons écrire

$$\sum_{K=0}^{m^{N+1}-1} \phi_K = \sum_{k=0}^{m^{N-1}} \sum_{\xi=0}^{m-1} \phi_{k+m^N \xi} \quad (53)$$

ce qui n'est en fait qu'un réarrangement des expressions ϕ_K sous le signe somme.

Et avec

$$\phi_K = \prod_{i=0}^N \phi_i(\alpha_i^K) \quad (54)$$

il vient

$$\begin{aligned} \phi_K &= \left[\prod_{i=0}^{N-1} \phi_i(\alpha_i^K) \right] \cdot \phi_N(\alpha_N^K) \\ &= \left[\prod_{i=0}^{N-1} \phi_i(\alpha_i^k) \right] \cdot \phi_N(\xi) \end{aligned}$$

En substituant cette expression de ϕ_K dans (53) il vient

$$\begin{aligned} \sum_{K=0}^{m^{N+1}-1} \prod_{i=0}^N \phi_i(\alpha_i^K) &= \sum_{K=0}^{m^{N+1}-1} \phi_K \\ &= \sum_{k=0}^{m^{N-1}} \sum_{\xi=0}^{m-1} \left[\left(\prod_{i=0}^{N-1} \phi_i(\alpha_i^k) \right) \cdot \phi_N(\xi) \right] \\ &= \sum_{k=0}^{m^{N-1}} \left(\prod_{i=0}^{N-1} \phi_i(\alpha_i^k) \right) \cdot \sum_{\xi=0}^{m-1} \phi_N(\xi) \\ &= \left(\sum_{k=0}^{m^{N-1}} \prod_{i=0}^{N-1} \phi_i(\alpha_i^k) \right) \cdot \sum_{\xi=0}^{m-1} \phi_N(\xi) \end{aligned}$$

et en vertu de (51), il vient

$$\begin{aligned} \sum_{K=0}^{m^{N+1}-1} \phi_K &= \left(\prod_{i=0}^{N-1} \sum_{q=0}^{m-1} \phi_i(q) \right) \cdot \sum_{\xi=0}^{m-1} \phi_N(\xi) \\ &= \prod_{i=0}^N \sum_{q=0}^{m-1} \phi_i(q) \end{aligned}$$

et (49) est vérifiée pour $n = N+1$, donc pour toutes les valeurs de n .

CHAPITRE V

POLYNOMES MODULO P.

PREMIÈRE PARTIE

Nous avons montré plus haut que l'on pouvait exprimer la fonction Identité à partir des fonctions somme et produit modulo m , pour $m = 2$ et $m = 3$.

Nous allons maintenant montrer que ce résultat peut s'étendre à un m premier quelconque.

LEMME 1

Pour $m = p$ (p premier), on a

$$I(a, b) = 1 + (p-1) \sum_{r=0}^{p-1} a^{p-1-r} b^r \pmod{p} \quad (55)$$

pour tout $0 \leq a, b \leq p-1$

En effet, considérons les quatre cas suivants :

1°) $a = b$

On a :

$$\begin{aligned} 1 + (p-1) \sum_{r=0}^{p-1} a^{p-1-r} b^r &= 1 + (p-1) \sum_{r=0}^{p-1} a^{p-1} \pmod{p} \\ &= 1 + (p-1) \cdot p \cdot a^{p-1} \pmod{p} \\ &= 1 \pmod{p} \end{aligned} \quad (56)$$

2°) $a = 0$ et $0 < b \leq p-1$.

On a :

$$1 + (p-1) \sum_{r=0}^{p-1} a^{p-1-r} b^r = 1 + (p-1) b^{p-1} \pmod{p} \quad (57)$$

Or, d'après le théorème de Fermat, $b^{p-1} = 1 \pmod{p}$

D'où :

$$1 + (p-1) \sum_{r=0}^{p-1} a^{p-1-r} b^r = 1 + (p-1) = 0 \pmod{p} \quad (58)$$

$$3^\circ) 0 < a \leq p-1 \text{ et } b = 0$$

L'expression (55) étant symétrique en a et b, ce cas se ramène au précédent.

$$4^\circ) 0 < a, b \leq p-1 \text{ et } a \neq b$$

On a :

$$\begin{aligned} 1 + (p-1) \sum_{r=0}^{p-1} a^{p-1-r} b^r &= 1 + (p-1) a^{p-1} \sum_{r=0}^{p-1} (a^{-1} b)^r \\ &= 1 + (p-1) \sum_{r=0}^{p-1} (a^{-1} b)^r \pmod{p} \\ &= 1 + (p-1) \frac{(a^{-1} b)^p - 1}{(a^{-1} b) - 1} \pmod{p} \\ &= 1 + (p-1) \frac{(a^{-1} b) - 1}{(a^{-1} b) - 1} \pmod{p} \\ &= 1 + p - 1 = 0 \pmod{p} \end{aligned} \quad (59)$$

Ce qui démontre le lemme.

THÉORÈME 2

L'ensemble de la somme modulo p et du produit modulo p est semi-fonctionnel.

En effet, d'après le premier théorème, l'ensemble de la somme modulo p, du produit modulo p et de la fonction identité est semi-fonctionnel. Or la fonction identité est exprimable explicitement à partir des deux premières. On en déduit que l'ensemble de celles-ci est semi-fonctionnel.

POLYNOME MODULO p

Nous avons vu plus haut, pour les cas $p = 2$ et $p = 3$, qu'en substituant à la fonction identité dans la forme canonique A son expression à partir de la somme et du produit modulo 2 et 3, on arrivait à une expression générale sous forme de polynome.

Il est clair que dans le cas général, pour p quelconque, le polynome ainsi obtenu sera de puissance p-1 en une variable quelconque, puisqu'en vertu du théorème de Fermat, toute puissance supérieure à p-1 d'une variable quelconque est congrue à une puissance inférieure ou égale à p-1 de cette variable.

Sous sa forme la plus générale le polynome modulo p sera une somme de produits affectés d'un coefficient résidu modulo p. Il y aura autant de

produits que de combinaisons différentes des variables élevées à toutes les puissances résidu modulo p.

Nous conviendrons d'écrire ce polynome sous la forme générale suivante :

$$(v_0, v_1, \dots, v_{n-1}) = \sum_{k=0}^{p^n-1} a_k \prod_{i=0}^{n-1} v_i^{\alpha_i^k} \quad \text{mod. } p \quad (60)$$

avec $0 \leq a_k \leq p-1$

et $k = \sum_{i=0}^{n-1} \alpha_i^k \cdot p^i$ (somme et produits arithmétiques)

c'est-à-dire, selon la notation adoptée plus haut, avec $\alpha_i^k = i^{\text{ème}}$ chiffre de k dans un système de numération de base p.

EXEMPLES :

1°) $p = 2$

a) $n = 1 \quad f(v_0) = a_0 + a_1 v_0 \quad \text{mod. } 2$

b) $n = 2 \quad f(v_0, v_1) = a_0 + a_1 v_0 + a_2 v_1 + a_3 v_0 v_1 \quad \text{mod. } 2$

c) $n = 3 \quad f(v_0, v_1, v_2) = a_0 + a_1 v_0 + a_2 v_1 + a_3 v_0 v_1 + a_4 v_2 + a_5 v_0 v_2 + a_6 v_1 v_2 + a_7 v_0 v_1 v_2 \quad \text{mod. } 2$

Nous pouvons maintenant construire, par exemple, une structure "universelle" à deux entrées, équivalente à celle décrite au chapitre précédent :

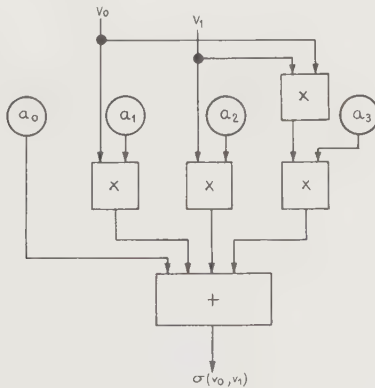


Fig. 22

Sur cette figure les combinateurs portant un signe X réalisent la fonction "Produit modulo 2", et celui portant un signe + la fonction "Somme modulo 2". Ce dernier peut se décomposer en une structure de plusieurs combinateurs à deux entrées, selon

$$a + b + c + d = a + (b + c + d) = a + [b + (c + d)] = \text{etc.} \quad \text{mod. } 2$$

La somme modulo 2 étant associative et commutative, l'ordre des entrées du combinateur "somme" de la figure 1 est sans importance.

Notons aussi que les deux combinateurs sur la droite de la figure 21 réalisant, ensemble, le produit $a_3 v_0 v_1$ peuvent être remplacés par un combinateur unique à trois entrées, réalisant le produit modulo 2 de celles-ci.

Le constructeur fixera les constantes a_0, a_1, a_2 et a_3 de l'une des 16 manières possibles, selon la fonction à réaliser.

Si les coefficients f_0, f_1, f_2 et f_3 du tableau de vérité sont connus, il faudra faire :

$$a_0 = f_0$$

$$a_1 = f_0 + f_1 \quad \text{mod. 2}$$

$$a_2 = f_0 + f_2 \quad \text{mod. 2}$$

$$\text{et} \quad a_3 = f_0 + f_1 + f_2 + f_3 \quad \text{mod. 2}$$

2°) $p = 3$

$$\text{a) } n = 1 \quad f(v_0) = a_0 + a_1 v_0 + a_2 v_0^2 \quad \text{mod 3}$$

$$\text{b) } n = 2 \quad f(v_0, v_1) = a_0 + a_1 v_0 + a_2 v_0^2 + a_3 v_1 + a_4 v_0 v_1 + a_5 v_0^2 v_1 + a_6 v_1^2 + a_7 v_0 v_1^2 + a_8 v_0^2 v_1^2 \quad \text{mod. 3}$$

Une structure universelle, réalisant une fonction quelconque d'une seule variable v_0 pourra être construite comme suit

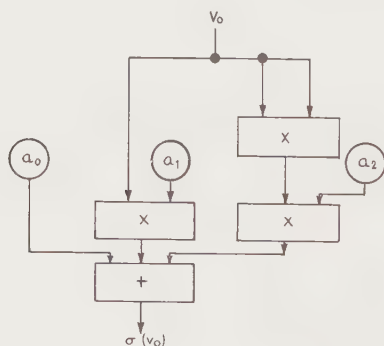


Fig. 23

Les combinateurs ci-dessus réalisent la somme et le produit modulo 3.

Notons que v_0^2 a été réalisé en connectant v_0 aux deux entrées d'un même combinateur produit.

On peut imaginer plusieurs structures équivalentes à celles de la figure 23, notamment en remplaçant les deux combinateurs produit réalisant ensemble

$$a_2 v_0^2$$

par un combinateur unique à trois entrées réalisant le produit de celles-ci (fig. 24)

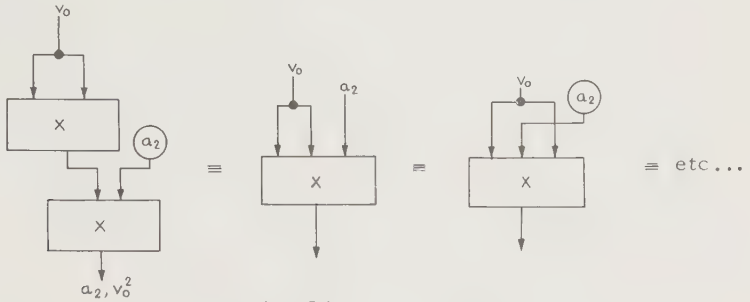


Fig. 24

Comme dans le cas précédent, le constructeur devra fixer les constantes a_0 , a_1 et a_2 en fonction des constantes f_0 , f_1 et f_2 du tableau de vérité, selon les relations suivantes :

$$\left. \begin{aligned} a_0 &= f_0 \\ a_1 &= 2 f_1 + f_2 \\ a_2 &= 2 (f_0 + f_1 + f_2) \end{aligned} \right\} \text{ mod. } 3$$

De façon générale, nous nous trouvons devant le problème suivant :

Etant donné une fonction, définie dans $E = (0, 1, \dots, n-1)$ par son tableau de vérité, exprimer celle-ci sous forme de polynome modulo p . En d'autres termes, étant donné le vecteur $\langle f_0, f_1, \dots, f_{p^n-1} \rangle$, de p^n éléments, calculer le vecteur $\langle a_0, a_1, \dots, a_{p^n-1} \rangle$ de p^n éléments, ceux-ci étant, dans l'ordre, les coefficients du polynome modulo p , dans la représentation (60).

Un moyen évident consiste à exprimer la fonction sous forme canonique, puis d'y substituer l'expression de $I(a, b)$ donnée au lemme 1, et enfin de grouper les termes semblables après y avoir remplacé les puissances supérieures à $p-1$ par les puissances congrues, inférieures à p . Mais ce moyen devient fastidieux si le nombre de variables est élevé. Nous indiquons dans ce qui suit une méthode matricielle comparativement simple.

Cas d'une variable unique

Soient q , r et t des résidus modulo p .

Considérons le polynome $f(v)$ modulo p en une variable unique v .

$$f(v) = \sum_{q=0}^{p-1} a_q v^q \quad \text{mod. } p \quad (61)$$

Soit f_r , la valeur de $f(v)$ pour $v = r$

$$\text{On a} \quad f_r = \sum_{q=0}^{p-1} a_q \cdot r^q \quad (62)$$

qui donne, sous forme matricielle,

$$\begin{pmatrix} f_0 \\ f_1 \\ \dots \\ f_r \\ \dots \\ f_{p-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & r & r^2 & \dots & r^{p-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & p-1 & (p-1)^2 & \dots & (p-1)^{p-1} \end{pmatrix} \times \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_q \\ \dots \\ a_{p-1} \end{pmatrix} \pmod{p}$$

Dénotons par A la matrice ci-dessus, et par A_{rq} son élément (ligne r colonne q). On a

$$A_{rq} = r^q \pmod{p} \quad (63)$$

Considérons maintenant le problème inverse :

Etant donné l'ensemble des valeurs prises par le polynôme :

$$\sum_{q=0}^{p-1} a_q v^q \pmod{p}$$

pour toutes les valeurs de v, en déterminer les coefficients a_q .

Ce problème se ramène évidemment à calculer la matrice inverse de A.

Ecrivons :

$$a_q = \sum_{t=0}^{p-1} B_{q,t} f_t \quad (64)$$

avec

$$B = A^{-1}$$

et

$B_{q,t}$ l'élément de B (ligne q colonne t)

LEMME 2

$$B_{q,t} = 1 - q^{p-1} - t^{p-1-q} \pmod{p} \quad (65)$$

En effet, considérons la matrice M (Elément M_{rt}), produit modulo p des matrices A et B :

$$M_{rt} = \sum_q A_{rq} \cdot B_{qt} \pmod{p} \quad (66)$$

$$= \sum_{q=0}^{p-1} r^q (1 - q^{p-1} - t^{p-1-q}) \pmod{p}$$

$$= \sum_{q=0}^{p-1} r^q (1 - q^{p-1}) - \sum_{q=0}^{p-1} r^q t^{p-1-q} \pmod{p}$$

$$= r^0 (1 - 0) + \sum_{q=1}^{p-1} r^q (1 - q^{p-1}) - \sum_{q=0}^{p-1} r^q t^{p-1-q} \pmod{p}$$

En vertu du théorème de Fermat, on a $q^{p-1} = 1 \pmod p$ pour

$$1 \leq q \leq p-1$$

Ce qui nous donne

$$M_{rt} = 1 - \sum_{q=0}^{p-1} r^q t^{p-1-q} \pmod p$$

En se reportant à la fonction Identité décrite plus haut, nous avons :

$$M_{rt} = I(r, t).$$

La matrice M est donc la matrice identité, et nous avons bien

$$B = A^{-1} \quad (67)$$

EXEMPLES

a) Pour $m = 2$

$$\begin{array}{ccc|ccc} & 1 & & 0 & & \\ & 1 & & 1 & & \\ \hline & & & & & \end{array} \quad \begin{array}{ccc|ccc} & 1 & & 0 & & \\ & 1 & & 1 & & \\ \hline & & & & & \end{array}$$

A B

La matrice A et son inverse sont identiques, et l'on a

$$\begin{array}{ll} a_0 = f_0 & f_0 = a_0 \\ a_1 = f_0 + f_1 \pmod 2 & f_1 = a_0 + a_1 \pmod 2 \end{array}$$

b) Pour $m = 3$

$$\begin{array}{ccc|ccc} & 1 & & 0 & & 0 \\ & 1 & & 1 & & 1 \\ & 1 & & 2 & & 1 \\ \hline & & & & & \end{array} \quad \begin{array}{ccc|ccc} & 1 & & 0 & & 0 \\ & 0 & & 2 & & 1 \\ & 2 & & 2 & & 2 \\ \hline & & & & & \end{array}$$

A B

$$\left. \begin{array}{ll} a_0 = f_0 & f_0 = a_0 \\ a_1 = 2f_1 + f_2 & f_1 = a_0 + a_1 + a_2 \\ a_2 = 2(f_1 + f_2 + f_3) & f_2 = a_0 + 2a_1 + a_2 \end{array} \right\} \pmod 3$$

La fonction "cyclage" de Post, par exemple, qui est donnée par

$$f_0 = 1 \quad f_1 = 2 \quad \text{et} \quad f_2 = 0 \quad \text{nous donne}$$

$$\begin{aligned} a_0 &= 1 \\ a_1 &= 2 \cdot 2 + 0 = 1 \pmod 3 \\ a_2 &= 2(1 + 2 + 0) = 0 \pmod 3 \end{aligned}$$

Donc :

$$f(v_0) = 1 + v_0 \pmod 3$$

Ce résultat est évident a priori, mais il illustre ici l'utilisation de la matrice B.

Cas de n variables

Nous passons maintenant au cas d'une fonction de n variables. Etant donné le vecteur $(f_0, f_1, \dots, f_{p^n-1})$ de p^n éléments, il s'agit de déterminer la matrice carrée, dont le produit modulo p avec ce vecteur donne le vecteur $(a_0, a_1, \dots, a_{p^n-1})$.

Nous allons démontrer que cette matrice est engendrée par la matrice B d'ordre p , selon une loi de composition dite "Produit de Fusion".

DEFINITION

Soient M et R deux matrices carrées d'ordre m et r respectivement.

On appelle Produit de Fusion de M par R , et l'on désigne par $M \otimes R$ la matrice carrée G d'ordre mr

$$G = M \otimes R = \begin{array}{|c|c|c|c|} \hline M.R_{0,0} & M.R_{0,1} & & M.R_{0,r-1} \\ \hline M.R_{1,0} & & & \\ \hline & & & \\ \hline M.R_{r-1,0} & & & M.R_{r-1,r-1} \\ \hline \end{array}$$

En d'autres termes

$$G_{k,j} = M_{\mu,\nu} \cdot R_{\rho,\sigma} \quad (68)$$

avec

$$0 \leq k, j \leq mr - 1 \quad (69)$$

$$0 \leq \mu, \nu \leq m - 1 \quad (70)$$

$$0 \leq \rho, \sigma \leq r - 1 \quad (71)$$

$$k = \mu + m\rho \quad (72)$$

$$\text{et} \quad j = \nu + m\sigma \quad (73)$$

L'élément $G_{k,j}$ de la matrice G est déterminé sans ambiguïté à partir des Matrices M et R , puisqu'à tout couple k, j correspondent deux et seulement deux couples μ, ρ et ν, σ satisfaisant les relations (69) à (73).

Si C est une matrice carrée d'ordre p , nous désignerons par C^2 le produit de fusion $C \otimes C \bmod p$, et de façon générale, nous écrirons

$$C^{n+1} = C^n \otimes C \bmod p \quad \text{pour tout } n \geq 1 \quad (74)$$

De ces définitions découle le résultat suivant avec $C^1 = C$

$$J_{k,j}^n = \prod_{i=0}^{n-1} C_{\alpha_i^k, \alpha_i^j} \bmod p \quad (75)$$

$C_{k,j}^n$ dénotant l'élément de la matrice carrée C^n (d'ordre p^n) situé à l'intersection de la ligne k et de la colonne j , avec

$\alpha_i^k = i^{\text{ème}}$ chiffre de k dans une numération de base p

$\alpha_i^j = i^{\text{ème}}$ chiffre de j dans une numération de base p

Nous démontrerons cette relation par récurrence sur n .

Pour $n = 1$, (75) devient

$$C_{k,j} = C_{\alpha_0^k, \alpha_0^j} \bmod p \quad (76)$$

En effet, nous avons dans ce cas

$$0 \leq k, j \leq p-1$$

et par conséquent

$$\alpha_0^k = k$$

$$\alpha_0^j = j$$

$$\text{et} \quad \alpha_i^k = \alpha_i^j = 0 \quad \text{pour tout} \quad i > 0$$

Supposons maintenant la relation (75) vérifiée pour une valeur N de n

$$C_{k,j}^N = \prod_{i=0}^{N-1} C_{\alpha_i^k, \alpha_i^j} \bmod p \quad (77)$$

avec

$$0 \leq k, j \leq p^N - 1, \quad p^N \text{ étant l'ordre de la matrice } C^N$$

Nous avons, par définition,

$$C^{N+1} = C^N \otimes C \bmod p$$

c'est-à-dire

$$C_{k+p^N q, j+p^N t}^{N+1} = C_{k,j}^N \cdot C_{q,t} \bmod p \quad (78)$$

avec

$$0 \leq q, t \leq p-1$$

Si nous posons maintenant

$$K = k + p^N q$$

$$\text{et} \quad J = j + p^N t$$

il vient

$$\alpha_i^K = \alpha_i^k \quad \text{pour tout } i \quad 0 \leq i \leq N-1$$

$$\text{et} \quad \alpha_N^K = q$$

De même

$$\alpha_i^J = \alpha_i^j \quad \text{pour tout } i \quad 0 \leq i \leq N-1$$

et $\alpha_N^J = t$

L'expression (78) nous donne donc

$$\begin{aligned} C_{K,J}^{N+1} &= \prod_{i=0}^{N-1} C_{\alpha_i^k, \alpha_i^j} \cdot C_{q,t} \\ &= \prod_{i=0}^{N-1} C_{\alpha_i^k, \alpha_i^j} \cdot C_{\alpha_N^k, \alpha_N^j} \pmod{p} \\ &= \prod_{i=0}^N C_{\alpha_i^k, \alpha_i^j} \end{aligned}$$

et la relation (75) est vérifiée pour $n = N + 1$, donc pour toutes les valeurs de $n \geq 1$.

EXEMPLES :

a) $m = 2$

$$B = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \quad B^2 = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{vmatrix}$$

b) $m = 3$

$$B = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{vmatrix} \quad B^2 = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ \hline 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix}$$

c) Pour p quelconque, nous avons vu que

$$I(k, j) = \prod_{i=0}^{n-1} I(\alpha_i^k, \alpha_i^j)$$

La matrice identité d'ordre p^n est donc la $n^{\text{ème}}$ puissance par rapport au produit de fusion (modulo p , ou tout autre produit) de la matrice identité d'ordre p .

Il découle aussi des définitions ci-dessus que l'inverse de la $n^{\text{ème}}$ puissance d'une matrice est la $n^{\text{ème}}$ puissance de l'inverse de cette matrice, par rapport au produit de fusion.

En d'autres termes

$$(C^n)^{-1} = (C^{-1})^n \quad (79)$$

En effet, désignons par D l'inverse de la matrice C et écrivons

$$C_{k,j}^n = \prod_{i=0}^{n-1} C_{\alpha_i^k, \alpha_i^j} \text{ mod } p \quad (80)$$

et

$$D_{j,e}^n = \prod_{i=0}^{n-1} D_{\alpha_i^j, \alpha_i^e} \text{ mod } p \quad (81)$$

Formons le produit

$$M = C^n \cdot D^n$$

c'est-à-dire

$$\begin{aligned} M_{k,e} &= \sum_{j=0}^{p^n-1} (C_{k,j}^n \cdot D_{j,e}^n) \text{ mod } p \\ &= \sum_{j=0}^{p^n-1} \prod_{i=0}^{n-1} (C_{\alpha_i^k, \alpha_i^j} \cdot D_{\alpha_i^j, \alpha_i^e}) \text{ mod } p \end{aligned}$$

Or, en vertu de la relation (49) du Chapitre IV, nous pouvons écrire

$$M_{k,e} = \prod_{i=0}^{n-1} \sum_{q=0}^{p-1} (C_{\alpha_i^k, q} \cdot D_{q, \alpha_i^e}) \text{ mod } p \quad (82)$$

Mais, par définition, nous avons

$$D = C^{-1}$$

qui nous donne

$$\sum_{q=0}^{p-1} (C_{\alpha_i^k, q} \cdot D_{q, \alpha_i^e}) = I(\alpha_i^k, \alpha_i^e) \quad (83)$$

En substituant dans (82), il vient :

$$M_{k,e} = \prod_{i=0}^{n-1} I(\alpha_i^k, \alpha_i^e) = I(k, e)$$

La matrice M est donc la matrice Identité d'ordre p^n , et D^n est bien l'inverse de C^n .

THEOREME 3

Si $((f))$ désigne le vecteur $(f_0, f_1, \dots, f_{p^n-1})$ et $((a))$ le vecteur $(a_0, a_1, \dots, a_{p^n-1})$, on a, pour n quelconque ≥ 1 ,

$$((a)) = B^n \cdot ((f)) \pmod{p} \quad (84)$$

avec

$$B_{q,t} = 1 - q^{p-1} - t^{p-1-q} \pmod{p} \quad \text{pour } 0 \leq q, t \leq p-1$$

En effet, considérons le polynôme (60)

$$f(v_0, v_1, \dots, v_{n-1}) = \sum_{k=0}^{p^n-1} a_k \prod_{i=0}^{n-1} v_i^{\alpha_i^k} \pmod{p}$$

Si f_j dénote la valeur de $f(v_0, v_1, \dots, v_{n-1})$ pour $V = j$, on peut écrire

$$f_j = \sum_{k=0}^{p^n-1} a_k \prod_{i=0}^{n-1} (\alpha_i^j)^{\alpha_i^k} \pmod{p} \quad (85)$$

ou, sous une forme matricielle

$$((f)) = \bar{A} \cdot ((a)) \pmod{p}$$

avec

$$\bar{A}_{j,k} = \prod_{i=0}^{n-1} (\alpha_i^j)^{\alpha_i^k} \pmod{p} \quad (86)$$

On a donc

$$\bar{A} = A^n, \quad \text{avec } A_{q,r} = q^r \pmod{p}$$

or, la matrice inverse de A est la matrice B , avec

$$B_{q,t} = 1 - q^{p-1} - t^{p-1-q} \pmod{p}$$

La matrice inverse de $\bar{A}$ est donc la matrice B^n , et l'on a bien

$$((a)) = B^n ((f)) \pmod{p}$$

EXEMPLES

a) Soit à exprimer sous forme de polynome modulo 2 la fonction de 3 variables dont les coefficients $(f_0, f_1, \dots, f_7)$ sont dans l'ordre

$$1 \ 1 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1.$$

Nous avons

$$\begin{array}{c|c|c|c|c}
 \begin{array}{c} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{array} & = & \begin{array}{cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} & \times & \begin{array}{c} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{array} \\
\end{array} \quad \text{mod. 2}$$

qui donne

k	a_k	$\prod v_i \alpha_i^k$
0 0 0	$a_0 = 1$	1
0 0 1	$a_1 = 0$	v_0
0 1 0	$a_2 = 1$	v_1
0 1 1	$a_3 = 1$	$v_0 v_1$
1 0 0	$a_4 = 0$	v_2
1 0 1	$a_5 = 1$	$v_0 v_2$
1 1 0	$a_6 = 1$	$v_1 v_2$
1 1 1	$a_7 = 0$	$v_0 v_1 v_2$

$$f(v_0, v_1, v_2) = 1 + v_1 + v_0 v_1 + v_0 v_2 + v_1 v_2 \quad \text{mod. 2}$$

Cette fonction peut être réalisée par la structure suivante :

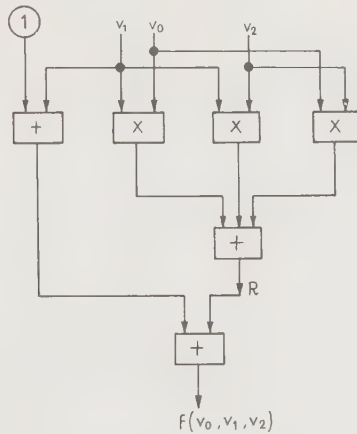


Fig. 25

LÉGENDE →

$$\begin{array}{c} a \quad b \\ \downarrow \quad \downarrow \\ \boxed{+} \\ \downarrow \\ a+b \text{ mod } 2 \end{array}$$

$$\begin{array}{c} a \quad b \quad c \\ \downarrow \quad \downarrow \quad \downarrow \\ \boxed{+} \\ \downarrow \\ a+b+c \text{ mod } 2 \\ = a+(b+c) \\ = \text{etc.} \end{array}$$

$$\begin{array}{c} a \quad b \\ \downarrow \quad \downarrow \\ \boxed{\times} \\ \downarrow \\ ab \text{ mod } 2 \end{array}$$

b) Soit à exprimer sous forme de polynome modulo 2 la fonction "Retenue" d'un additionneur binaire à trois entrées.

La retenue est égale à 1 si et seulement si plus d'une entrée est égale à 1.

Le tableau de vérité est le suivant :

v_2	v_1	v_0	R
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Ceci nous donne :

k	$\prod v_i \alpha_i^k$	a_k
0 0 0	1	0
0 0 1	v_0	0
0 1 0	v_1	0
0 1 1	$v_0 v_1$	1
1 0 0	v_2	0
1 0 1	$v_0 v_2$	1
1 1 0	$v_1 v_2$	1
1 1 1	$v_0 v_1 v_2$	0

$$r = v_0 v_1 + v_0 v_2 + v_1 v_2 \mod. 2$$

R peut être réalisée par une structure qui serait la sous structure aboutissant en R de la figure 25.

c) Soit à réaliser un additionneur "binaire complet", c'est-à-dire une structure à trois entrées : le i^{ème} chiffre binaire d'un nombre a, le i^{ème} chiffre binaire d'un nombre b, la retenue sur la somme des (i-1)^{èmes} chiffres de a et de b et dont les deux sorties sont :

la somme modulo 2 des trois entrées,
la retenue.

Cette structure peut être ainsi réalisée :

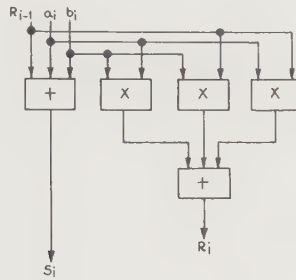


Fig. 26

d) Construire un "additionneur ternaire complet".

Comme dans l'exemple précédent, il nous faut réaliser :

1) La somme $a_i + b_i + R_{i-1} \pmod{3}$

et 2) La retenue R_i .

Le tableau de vérité de R_i est donné par :

R_{i-1}	b_i	a_i	S_i	R_i
0	0	0	0	0
0	0	1	1	0
0	0	2	2	0
0	1	0	1	0
0	1	1	2	0
0	1	2	0	1
0	2	0	2	0
0	2	1	0	1
0	2	2	1	1
1	0	0	1	0
1	0	1	2	0
1	0	2	0	1
1	1	0	2	0
1	1	1	0	1
1	1	2	1	1
1	2	0	0	1
1	2	1	1	1
1	2	2	2	1
2	0	0	2	0
2	0	1	0	1
2	0	2	1	1
2	1	0	0	1
2	1	1	1	1
2	1	2	2	1
2	2	0	1	1
2	2	1	2	1
2	2	2	0	2

La matrice B^3 est la suivante :

1 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 2 1	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
2 2 2	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	2 0 0	1 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 1 2	0 2 1	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	1 1 1	2 2 2	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
2 0 0	2 0 0	2 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 1 2	0 1 2	0 1 2	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
1 1 1	1 1 1	1 1 1	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	2 0 0	0 0 0	0 0 0	0 0 0	1 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	0 1 2	0 0 0	0 0 0	0 0 0	0 2 1	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	1 1 1	0 0 0	0 0 0	0 0 0	2 2 2	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	0 0 0	1 0 0	2 0 0	0 0 0	2 0 0	1 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	0 0 0	0 2 1	0 1 2	0 0 0	0 1 2	0 2 1	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	0 0 0	2 2 2	1 1 1	0 0 0	1 1 1	2 2 2	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	1 0 0	1 0 0	1 0 0	2 0 0	2 0 0	2 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	0 2 1	0 2 1	0 2 1	0 1 2	0 1 2	0 1 2	0 0 0	0 0 0	0 0 0
0 0 0	0 0 0	0 0 0	2 2 2	2 2 2	2 2 2	1 1 1	1 1 1	1 1 1	0 0 0	0 0 0	0 0 0
2 0 0	0 0 0	0 0 0	2 0 0	0 0 0	0 0 0	2 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 1 2	0 0 0	0 0 0	0 1 2	0 0 0	0 0 0	0 1 2	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
1 1 1	0 0 0	0 0 0	1 1 1	0 0 0	0 0 0	1 1 1	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	1 0 0	2 0 0	0 0 0	1 0 0	2 0 0	0 0 0	1 0 0	2 0 0	0 0 0	0 0 0	0 0 0
0 0 0	0 2 1	0 1 2	0 0 0	0 2 1	0 1 2	0 0 0	0 2 1	0 1 2	0 0 0	0 0 0	0 0 0
0 0 0	2 2 2	1 1 1	0 0 0	2 2 2	1 1 1	0 0 0	2 2 2	1 1 1	0 0 0	0 0 0	0 0 0
1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0	1 0 0
0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1	0 2 1
2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2	2 2 2

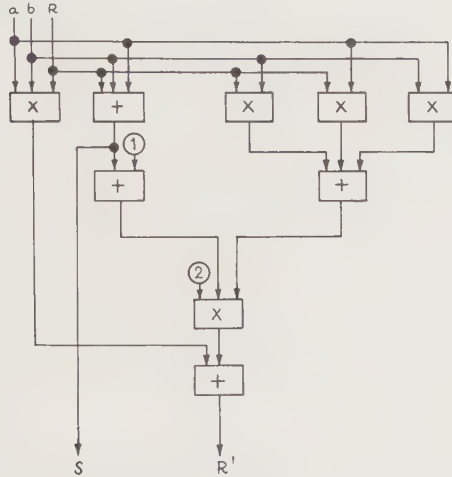
qui nous donne, en remplaçant a_i , b_i , R_{i-1} et R_i par a , b , R et R' pour simplifier l'écriture :

$$R' = 2[(ab + aR + bR) + a^2b + a^2R + b^2a + b^2R + R^2a + R^2b] + abR \quad \text{mod. } 3$$

Ceci s'écrit plus simplement :

$$R' = 2(ab + aR + bR)(1 + a + b + R) + abR.$$

Et l'on obtient la structure :



Noter que S la somme Modulo 3, est la sortie d'une sous-structure de la structure ci-dessus.

DEUXIÈME PARTIE

Il est bien connu qu'un polynome de degré n en x prenant des valeurs entières pour des valeurs entières de x peut être écrit sous la forme :

$$f(x) = b_0 + b_1 \binom{x}{1} + b_2 \binom{x}{2} + \dots + b_n \binom{x}{n} \quad (87)$$

$$\binom{x}{j} = C_x^j = \frac{x!}{(x-j)! j!} \quad \begin{aligned} \binom{x}{0} &= 1 \text{ pour } x \geq 0 \\ \binom{x}{j} &= 0 \text{ pour } x < j \end{aligned} \quad (88)$$

et des coefficients $b_0, b_1 \dots b_n$ entiers.

Nous avons vu au chapitre précédent qu'une fonction de commutation quelconque, à p valeurs, de v_0 , pouvait être représentée par un polynome modulo p de degré $p-1$ en v_0 .

Cette fonction pourra donc être écrite sous la forme :

$$f(v_0) = b_0 + b_1 \binom{v_0}{1} + b_2 \binom{v_0}{2} + \dots + b_{p-1} \binom{v_0}{p-1} \text{ mod. } p \quad (89)$$

De façon générale, une fonction de commutation de n variables $v_0, v_1 \dots v_{n-1}$ pourra être représentée sous forme d'une somme modulo p de p termes, chaque terme étant le produit modulo p de n coefficients du binôme $\binom{v_i}{a_i}$, affectés d'un coefficient constant, résidu modulo p .

Nous conviendrons d'écrire, sous forme générale :

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{g=0}^{p^n-1} b_g \prod_{i=0}^{n-1} \binom{v_i}{\alpha_i^g} \mod. p \quad (90)$$

avec g entier $0 \leq g \leq p^n-1$

EXEMPLES

a) $p = 3$ $n = 1$

$$f(v_0) = b_0 + b_1 \binom{v_0}{1} + b_2 \binom{v_0}{2} \mod. 3 \quad (91)$$

b) $p = 2$ $n = 2$

$$f(v_0, v_1) = b_0 + b_1 \binom{v_0}{1} \binom{v_1}{0} + b_2 \binom{v_0}{0} \binom{v_1}{1} + b_3 \binom{v_0}{1} \binom{v_1}{1} \mod. 2 \quad (92)$$

Notons que, de façon générale :

$$\binom{v}{0} = 1 \quad \text{pour tout } v \geq 0$$

$$\text{et } \binom{v}{1} = v \quad \text{pour tout } v$$

L'expression ci-dessus se ramène par conséquent à :

$$f(v_0, v_1) = b_0 + b_1 v_0 + b_2 v_1 + b_3 v_0 v_1$$

Celle-ci est identique au polynome modulo 2 du chapitre précédent (pour $p = 2$, $a_i = b_i$ pour toutes les valeurs de i).

Le problème de synthèse d'une structure, en fonction de combinateurs hypothétiques réalisant la fonction $\binom{v}{a}$, la somme et le produit modulo p , se ramène donc ici à calculer les coefficients $b_0, b_1 \dots b_{p^n-1}$ à partir des coefficients $f_0, f_1 \dots f_{p^n-1}$ du tableau de vérité.

Nous étudions dans ce qui suit une matrice particulière, permettant cette transformation.

Ce chapitre est basé sur un théorème fondamental, dû à Lucas, et qui a été retrouvé par l'auteur, alors que celui-ci ignorait l'existence de ce théorème.

THEOREME DE LUCAS 18

Soit α_i^x le $i^{\text{ème}}$ chiffre de x dans un système de numération de base p ,
et α_i^y " " " " " " " "
avec p premier,

On a :

$$\binom{x}{y} = \prod_{i=0}^{\infty} \binom{\alpha_i^x}{\alpha_i^y} \text{ modulo } p \quad (93)$$

DEFINITION

Si q est un entier $0 \leq q \leq p-1$

nous appelons "complément de q à $p-1$ ", et nous dénotons par $\bar{q}$

$$\bar{q} = (p-1) - q \quad (94)$$

De même si g est un entier $0 \leq g \leq p^n-1$

nous appelons complément de g à p^n-1 , et nous dénotons par g'

$$g' = (p^n-1) - g \quad (95)$$

Notons que

$$g' = \bar{g} \quad \text{mod. } p$$

COROLLAIRE 1

Pour $0 \leq x, y \leq p^n-1$

On a :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \prod_{i=0}^{n-1} \begin{pmatrix} \bar{\alpha}_i^x \\ \bar{\alpha}_i^y \end{pmatrix} \quad \text{mod. } p \quad (96)$$

En effet, si α_i^x représente le $i^{\text{ème}}$ chiffre de x dans un système de numération de base p , le $i^{\text{ème}}$ chiffre de $(p^n-1) - x$ est $(p-1) - \alpha_i^x$, c'est-à-dire $\bar{\alpha}_i^x$, puisque :

$$\sum_{i=0}^{n-1} \bar{\alpha}_i^x \cdot p^i = \sum_{i=0}^{n-1} [(p-1) - \alpha_i^x] p^i = \sum_{i=0}^{n-1} (p-1) \cdot p^i - \sum_{i=0}^{n-1} \alpha_i^x p^i = (p^n-1) - x = x'$$

COROLLAIRE 2

Pour $0 \leq a, b \leq p-1$

On a :

$$I(a, b) = \sum_{q=0}^{p-1} \begin{pmatrix} \bar{a} \\ \bar{q} \end{pmatrix} \begin{pmatrix} b \\ q \end{pmatrix} \quad \text{mod. } p \quad (97)$$

En effet, il est démontré que pour a, b et r entiers :

$$\sum_q \begin{pmatrix} r \\ q-a \end{pmatrix} \begin{pmatrix} b \\ q \end{pmatrix} = \begin{pmatrix} r+b \\ r+a \end{pmatrix} \quad (98)$$

Or, il est bien connu que $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ x-y \end{pmatrix}$, ce qui nous donne :

$$\begin{pmatrix} r \\ q-a \end{pmatrix} = \begin{pmatrix} r \\ r-q+a \end{pmatrix} \quad (99)$$

(98) devient par conséquent :

$$\sum_q \begin{pmatrix} r \\ r-q+a \end{pmatrix} \begin{pmatrix} b \\ q \end{pmatrix} = \begin{pmatrix} r+b \\ r+a \end{pmatrix}$$

Or, en posant $a + r = p - 1$, il vient :

$$\sum_q \binom{p-1-a}{p-1-q} \binom{b}{q} = \binom{r+b}{r+a} = \binom{p-1-a+b}{p-1} = \binom{p-1-(a-b)}{p-1}$$

Par conséquent :

$$\sum_{q=0}^{p-1} \binom{\bar{a}}{\bar{q}} \binom{b}{q} = \binom{p-1-(a-b)}{p-1} \pmod{p}$$

En posant $p - 1 - (a - b) = c$

il vient :

$$\sum_{q=0}^{p-1} \binom{\bar{a}}{\bar{q}} \binom{b}{q} = \binom{c}{p-1} \pmod{p}$$

1er Cas : $a = b$, donc $c = p - 1$

et $\binom{c}{p-1} = 1$

2e Cas : $a > b$, donc $c < p - 1$

et $\binom{c}{p-1} = 0$

3e Cas : $a < b$, donc $2(p-1) \geq c > p-1$

et nous avons, d'une part $\alpha_0^{p-1} = p-1$

et $\alpha_i^{p-1} = 0$ pour tout $i > 0$

et d'autre part $\alpha_0^c \leq p-2$

$$\alpha_1^c = 1$$

$$\alpha_i^c = 0 \quad \text{pour tout } i > 1$$

On a donc, en vertu du théorème de Lucas,

$$\begin{aligned} \binom{c}{p-1} &= \binom{\alpha_0^c}{p-1} \binom{1}{0} \cdot \prod_{i=2}^{\infty} \binom{0}{0} \pmod{p} \\ &= 0 \pmod{p} \end{aligned}$$

Ce qui démontre le corollaire.

COROLLAIRE 3

Pour $0 \leq x, y \leq p^n - 1$

$$I(x, y) = \sum_{j=0}^{p^n-1} \binom{x'_j}{j} \binom{y}{j} \pmod{p} \quad (100)$$

En effet :

$$\begin{aligned}
 I(x, y) &= \prod_{i=0}^{n-1} (I(\alpha_i^x, \alpha_i^y) \text{ par définition}) \\
 &= \prod_{i=0}^{n-1} \left[\sum_{q=0}^{p-1} \left(\frac{\bar{\alpha}_i^x}{\bar{\alpha}_i} \right) \left(\frac{\alpha_i^y}{\alpha_i^q} \right) \right] \text{ mod. } p \\
 &= \sum_{j=0}^{p^n-1} \left[\prod_{i=0}^{n-1} \left(\frac{\bar{\alpha}_i^x}{\bar{\alpha}_i} \right) \left(\frac{\alpha_i^y}{\alpha_i^j} \right) \right] \\
 &= \sum_{j=0}^{p^n-1} \left(x_{j'}^1 \right) \left(y_j \right) \text{ mod. } p
 \end{aligned}$$

THEOREME 4

Les coefficients $b_0, b_1 \dots b_{p^n-1}$ de l'expansion

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{g=0}^{p^n-1} \left[b_g \cdot \prod_{i=0}^{n-1} \left(\frac{v_i}{\alpha_i^g} \right) \right] \text{ mod. } p$$

sont obtenus à partir des coefficients $f_0, f_1 \dots f_{p^n-1}$ du tableau de vérité de la fonction f par la relation

$$b_g = \sum_{j=0}^{p^n-1} \left[f_j \cdot \left(\frac{j'}{g'} \right) \right] \text{ mod. } p$$

En effet, considérons l'expression :

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{g=0}^{p^n-1} b_g \prod_{i=0}^{n-1} \left(\frac{v_i}{\alpha_i^g} \right) \text{ mod. } p$$

Notons qu'en vertu du théorème de Lucas, nous pouvons écrire :

$$\prod_{i=0}^{n-1} \left(\frac{v_i}{\alpha_i^g} \right) = \left(\frac{V}{g} \right) \text{ mod. } p$$

D'où l'expression remarquable de f :

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{g=0}^{p^n-1} b_g \left(\frac{V}{g} \right) \text{ mod. } p \quad (101)$$

Revenons maintenant à la forme canonique A

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{j=0}^{p^n-1} f_j \cdot I(j, V) \quad (102)$$

que nous pouvons écrire, en vertu du Corollaire 3

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{j=0}^{p^{n-1}} \left[f_j \sum_{g=0}^{p^{n-1}} \binom{j'}{g'} \binom{V}{g} \right] \text{ mod. } p \quad (103)$$

expression obtenue à partir de (102), en effectuant la substitution

$$I(j, V) = \sum_{g=0}^{p^{n-1}} \binom{j'}{g'} \binom{V}{g} \text{ mod. } p$$

L'expression (103) peut s'écrire :

$$f(v_0, v_1 \dots v_{n-1}) = \sum_{g=0}^{p^{n-1}} \sum_{j=0}^{p^{n-1}} f_j \binom{j'}{g'} \binom{V}{g} \text{ mod. } p \quad (104)$$

En comparant les expressions (104) et (101), il vient :

$$bg = \sum_{j=0}^{p^{n-1}} f_j \binom{j'}{g'} \text{ mod. } p$$

C.Q.F.D.

EXEMPLES

La relation

$$bg = \sum_{j=0}^{p^{n-1}} f_j \cdot \binom{j'}{g'} \text{ mod. } p$$

s'écrit, sous forme matricielle

$$\begin{vmatrix} b_0 \\ b_1 \\ \dots \\ b_g \\ \dots \\ b_{p^{n-1}} \end{vmatrix} = M \begin{vmatrix} f_0 \\ f_1 \\ \dots \\ f_j \\ \dots \\ f_{p^{n-1}} \end{vmatrix} \text{ mod. } p$$

avec $M_{gj} = \binom{j'}{g'}$

M_{gj} étant l'élément situé à l'intersection de la ligne g et de la colonne j de la matrice M .

En vertu du corollaire 10, nous pouvons écrire :

$$\binom{j'}{g'} = \prod_{i=0}^{n-1} \binom{j_i}{g_i} \text{ mod. } p$$

Si l'on dénote par D la matrice d'ordre p telle que

$$D_{qt} = \binom{q_i}{t_i} \text{ mod. } p,$$

D_{qt} étant l'élément situé à l'intersection de la ligne q et de la colonne t de la matrice D, il vient

$$M = D^n \quad \text{mod. } p$$

(M est la n^{ième} puissance de D modulo p, par rapport au produit de Fusion).

Pour p = 2, nous avons

$$D = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}$$

Pour p = 3

$$D = \begin{vmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix}$$

Pour p = 5

$$\begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 4 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 4 & 3 & 2 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{vmatrix}$$

Soit à exprimer sous la forme (90) la fonction de 2 variables v_0 et v_1 définie dans $E = (0 \ 1 \ 2)$ dont les coefficients $f_0, f_1 \dots f_8$ sont, dans l'ordre

$$1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 2 \ 1$$

$$\begin{vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \end{vmatrix} \equiv \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{vmatrix} \times \begin{vmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 2 \\ 1 \end{vmatrix} \quad \text{mod. } 3$$

Les coefficients b_g sont donc, dans l'ordre

$$1 \ 2 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1$$

et l'on a :

$$f(v_0, v_1) = 1 + 2 v_0 + \binom{v_0}{2} + v_1 v_0 + v_1 \binom{v_0}{2} + \binom{v_1}{2} \binom{v_0}{2} \quad \text{mod. } 3$$

CHAPITRE VI

GÉNÉRALISATION DE LA FONCTION DE WEBB

En 1935, D.L. Webb [15] a démontré que l'opération ainsi définie

$$W(x, y) = 0 \quad \text{pour } x \neq y$$

$$= x+1 \text{ mod. } m \quad \text{pour } x = y, \quad x, y \in E$$

est fonctionnelle dans l'ensemble $E = (0, 1, \dots, m-1)$.

CYCLAGE

Considérons dans l'ensemble $E = (0, 1, \dots, m-1)$ la substitution t faisant correspondre à l'élément a de E , l'élément a^1 de E . A la permutation $0 \ 1 \ 2 \ \dots \ m-1$, la substitution t fait correspondre la permutation $0^1 \ 1^1 \ 2^1 \ \dots \ (m-1)^1$. La composition de deux substitutions t fait correspondre à l'élément a l'élément $(a^1)^1$, que nous écrirons a^2 . De façon générale la composition de q substitutions t (substitution t^q) fait correspondre à la permutation naturelle $0 \ 1 \ 2 \ \dots \ m-1$ la permutation $0^q \ 1^q \ \dots \ (m-1)^q$.

En d'autres termes, nous écrirons $(a^q)^1 = a^{q+1}$, avec $a^0 = a$. Nous appelons une substitution "cyclage" si pour i entier, on a

$$a^i = a \quad \text{pour } i \equiv 0 \text{ mod } m$$

$$a^i \neq a \quad \text{pour } i \not\equiv 0 \text{ mod } m \quad \text{pour tout } a \in E$$

Il en découle que si q et r dénotent des résidus modulo m

$$a^q = a^r \quad \text{si et seulement si } q = r \quad \text{pour tout } a \in E$$

$$a^q = b^q \quad \text{si et seulement si } a = b \quad \text{pour tout } q \in E$$

et, pour tout a et $b \in E$ il existe un élément q de E et un seul tel que :

$$a^q = b$$

Nous appelons q "distance" de a à b pour un cyclage t , et nous écrirons

$$a = \delta_{ab}$$

Pour tout $a \in E$, la suite

$$a \ a^1 \ a^2 \ \dots \ a^{m-1}$$

est une permutation des éléments de E , et définit entièrement le cyclage t .

En particulier, nous appelons la permutation

$$0 \ 0^1 \ 0^2 \ \dots \ 0^{m-1}$$

"permutation caractéristique" du cyclage t .

Notons qu'un cyclage t engendre un groupe cyclique d'ordre m par rapport à la composition des substitutions.

EXEMPLES

a) La substitution
$$t = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \end{pmatrix}$$

est un cyclage dont la permutation caractéristique est

$$0 \ 1 \ 3 \ 2$$

Ce cyclage peut aussi être caractérisé par le diagramme



b) La substitution
$$t = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

n'est pas un cyclage. Elle comprend deux cycles internes



et



c) La permutation circulaire de r rangs $(a + r \bmod m)$ n'est un cyclage que si r est premier à m .

En effet, soit

$$a^1 = a + r \bmod m$$

si $(r, m) > 1$ il existe un $\alpha \neq 0 \bmod m$ tel que

$$\alpha r \equiv 0 \bmod m, \text{ donc } a^\alpha = a + \alpha r \equiv a \bmod m$$

Il en découle que, quel que soit m , une permutation circulaire d'un rang (ou de $m-1$ rangs) est un cyclage, et, si m est premier, toute permutation circulaire est un cyclage.

De façon générale, si t est un cyclage, la substitution t^r est un cyclage si et seulement si $(r, m) = 1$.

Précisons enfin que le nombre de cyclages possibles dans un ensemble E de m éléments est $(m-1)!$ En effet, il y a autant de cyclages possibles que de permutations caractéristiques, c'est-à-dire de permutations de m éléments de E ayant un zéro à gauche, donc de permutations de $(m-1)$ éléments.

LA FONCTION G , Généralisation de la fonction W .

Nous introduisons maintenant la fonction suivante :

$$\begin{aligned} G(x, y) &= c && \text{pour tout } x, y \in E && x \neq y \\ G(x, y) &= x^1 && \text{pour } && x = y \end{aligned}$$

c étant un élément quelconque de E , et x^1 dénotant un cyclage quelconque de x .

(Remarquons que le fait de dire "cyclage de x " confond, par un abus de langage, l'opération "cyclage" et le résultat de celle-ci.)

Nous démontrons dans ce qui suit que l'opération G est fonctionnelle, quelle que soit la constante c et quel que soit le cyclage t choisi.

Si l'opération G porte sur deux arguments toujours égaux, nous avons :

$$G(x, x) = x^1$$

$$\text{De même} \quad G(y, y) = y^1.$$

Considérons maintenant une opération G portant sur les arguments x^1 et y^1 . Nous avons :

$$\begin{aligned} G(x^1, y^1) &= x^2 && \text{si } x = y \\ &= c && \text{si } x \neq y. \end{aligned}$$

De façon générale :

$$\begin{aligned} G(x^{q-1}, y^{q-1}) &= x^q && \text{si } x = y \\ &= c && \text{si } x \neq y. \end{aligned}$$

La fonction de x et y ainsi engendrée à partir de l'opération G sera dénotée par le symbole

$$G_{c,q}(x, y) \quad c, q \in E$$

Et la fonction G elle-même pourra s'écrire

$$G_{c,1}(x, y)$$

Schématiquement nous représenterons l'opération G par le combinateur de la figure 26

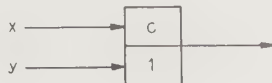


Fig. 26

et l'opération $G_{c,q}$ par le combinateur de la figure 27

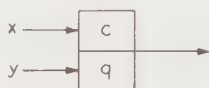


Fig. 27

Et nous avons l'équivalence

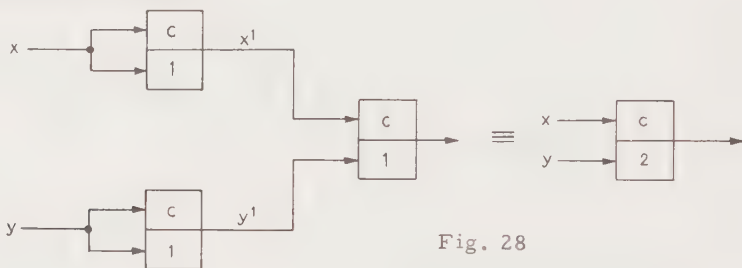


Fig. 28

Dans ce qui suit, nous aurons plus souvent recours à la représentation schématique des constructions qu'à leur expression algébrique, étant donné la grande simplicité relative de la première.

LEMME 3

L'opération $G_{c,1}$, avec c quelconque, engendre l'opération $G_{r,s}$ avec $r, s \in E$ quelconques.

En effet, nous avons vu plus haut que $G_{c,1}$ engendrait $G_{c,q}$ avec q quelconque.

Considérons maintenant la construction suivante :



Fig. 29

Les deux entrées du combinateur de droite sont identiques. Celles-ci sont égales à

$$\begin{array}{ll} x^q & \text{si } x = y \\ \text{et } c & \text{si } x \neq y \end{array}$$

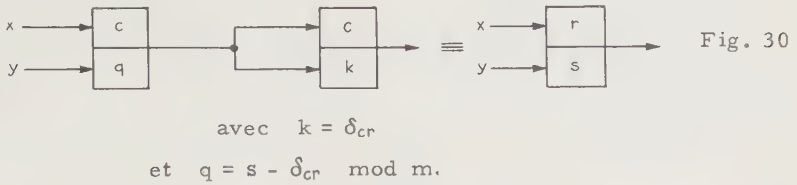
La sortie est par conséquent

$$\begin{array}{ll} z = x^{q+k} & \text{si } x = y \\ \text{et } z = c^k & \text{si } x \neq y \end{array}$$

Quelles que soient les valeurs prescrites de r et s , il existe toujours un k et un q satisfaisant :

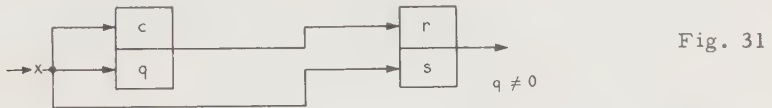
$$\begin{array}{ll} \delta_{cr} = k & (\text{c'est-à-dire } c^k = r) \\ \text{et } q+k \equiv s & \text{mod } m \end{array}$$

Et l'on a l'équivalence



LEMME 4

L'opération G engendre toutes les fonctions constantes (d'une variable). En effet, considérons la construction suivante :



L'entrée supérieure du combinateur G_{rs} est égale à x^q et son entrée inférieure à x . Ces deux entrées sont donc toujours différentes et la sortie est par conséquent r .

DEFINITION

Nous disons d'une fonction qu'elle a h "valeurs strictes" si elle prend exactement h valeurs.

Nous dénoterons par P_h la classe des fonctions d'une seule variable de h valeurs strictes, et par $\mathcal{P}_h$ l'ensemble $\bigcup_{i=1}^h P_i$ des fonctions d'une variable à h valeurs strictes ou moins.

LEMME 5

L'opération G engendre l'ensemble $\mathcal{P}_2$.

Nous avons vu au lemme 2 que G engendre P_1 (la classe des constantes). Il reste donc à démontrer que G engendre la classe P_2 .

Soit $f(x)$ une fonction quelconque de x appartenant à P_2 et prenant les valeurs a_1 et a_2 . Partitionnons l'ensemble E en 2 classes J_1 et J_2 telles que

$$\begin{aligned} f(j) &= a_1 && \text{pour tout } j \in J_1 \\ \text{et } f(j) &= a_2 && \text{pour tout } j \in J_2 \end{aligned}$$

et désignons les éléments de J_1 , rangés dans un ordre quelconque, par

$$J_1 = (j_1, j_2, \dots, j_\alpha)$$

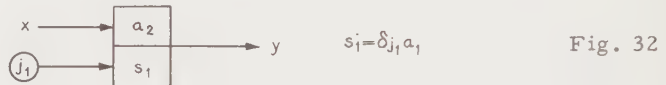
et ceux de J_2 par

$$J_2 = (j_{\alpha+1}, j_{\alpha+2}, \dots, j_m)$$

Nous démontrons alors le lemme par récurrence sur α .

a) Soit $\alpha = 1$

Il s'agit de réaliser la fonction $f(x)$ prenant la valeur a_1 pour $x = j_1$ et la valeur a_2 pour toute autre valeur de x . Considérons l'assemblage de la figure 32 :



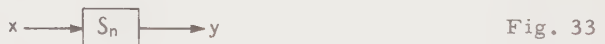
L'entrée inférieure du combinateur G_{a_2, s_1} ci-dessus est une constante égale à j_1 (obtenue par une structure semblable à celle décrite au lemme 2). Pour $x \neq j_1$, $y = a_2$ et pour $x = j_1$, $y = a_1$ et l'on a bien $y = f(x)$.

b) Supposons maintenant le lemme démontré pour $\alpha = n$, et soit à réaliser la fonction $f(x)$ telle que

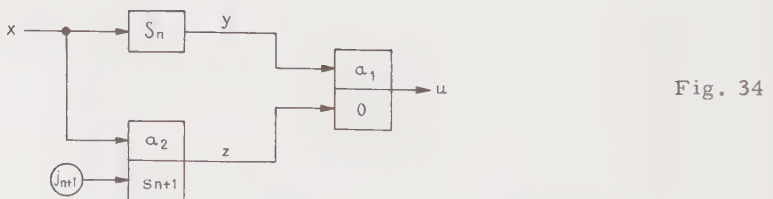
$$\begin{aligned} f(x) &= a_1 & \text{pour } x &= j_i & 1 \leq i \leq n+1 \\ \text{et } f(x) &= a_2 & \text{pour } x &= j_i & i > n+1 \end{aligned}$$

Le lemme étant supposé démontré pour $\alpha = n$, nous disposons (fig. 33) d'une fonction $S_n(x)$ satisfaisant

$$\begin{aligned} y = S_n(x) &= a_1 & \text{pour } x &= j_i & 1 \leq i \leq n \\ &= a_2 & \text{pour } x &= j_i & i > n \end{aligned}$$



Construisons la structure de la figure 34



La sortie z du combinateur $G_{a_2, s_{n+1}}$ est donnée par

$$\begin{aligned} z &= a_2 & \text{pour } x &= j_i & i \neq n+1 \\ &= a_1 & \text{pour } x &= j_{n+1} & \text{à condition de faire } \delta_{j_{n+1}, a_1} = s_{n+1} \end{aligned}$$

Et l'on a à la sortie du combinateur $G_{a_1,0}$

pour	$1 \leq i \leq n$	$y = a_1$ et $z = a_2$	donc	$u = a_1$
pour	$i = n+1$	$y = a_2$ et $z = a_1$	donc	$u = a_1$
pour	$i > n+1$	$y = a_2$ et $z = a_2$	donc	$u = a_2^2 = a_2$

Le lemme est donc démontré pour la valeur $n+1$ de α , et par conséquent pour toutes les valeurs de α .

LEMME 6

L'opération G engendre l'ensemble $\mathcal{G}_m$.

Autrement dit, G engendre toutes les fonctions d'une seule variable. Nous démontrerons ce lemme par récurrence sur h , l'indice de $\mathcal{G}_h$.

a) $h = 1$ - voir lemme 4

b) Supposons le lemme démontré pour une valeur n de h . En d'autres termes, supposons que nous disposions de structures capables de réaliser toutes les fonctions de n valeurs strictes, ou moins, d'une seule variable.

Il s'agit de démontrer que l'on peut engendrer à partir de l'ensemble $\mathcal{G}_n$ et de la fonction G une fonction quelconque $f(x)$ de la classe P_{n+1} .

Dénotons par $a_1, a_2, \dots, a_i, \dots, a_{n+1}$ les valeurs prises par $f(x)$, et par J_i la classe de toutes les valeurs de x auxquelles correspond la valeur a_i de x , avec $i = 1, 2 \dots n+1$.

Nous disposons par hypothèse de toutes les fonctions de la classe P_n et, en particulier, des fonctions $g(x)$ et $h(x)$ définies comme suit :

$$\begin{aligned} g(x) &= h(x) = a_i & \text{pour } x \in J_i & \quad i = 1, 2, \dots, n \\ g(x) &= a_v & \text{pour } x \in J_{n+1} & \quad \text{avec } v \leq n \\ h(x) &= a_\mu & \text{pour } x \in J_{n+1} & \quad \text{avec } \mu \leq n \text{ et } \mu \neq v \end{aligned}$$

Considérons maintenant la structure suivante :

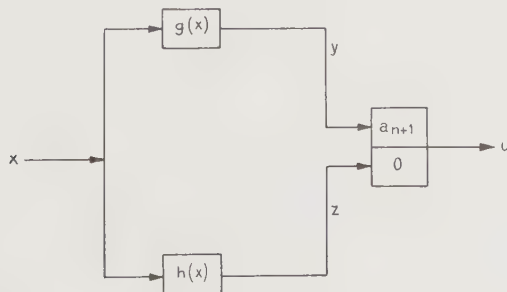


Fig. 35

La sortie u du combinateur $G_{a_{n+1}, 0}$ est donnée par ce qui suit :

Pour $x \in J_i$; $i = 1, 2 \dots n$ $y = z = a_i$ donc $u = a_i^0 = a_i$

Pour $x \in J_{n+1}$ $y = a_v$ et $z = a_\mu$, donc $y \neq z$ et $u = a_{n+1}$.

La récurrence n'est donc établie qu'à condition de pouvoir satisfaire $\mu \neq v$, c'est-à-dire pour toute valeur de n supérieure ou égale à 2. Pour $n = 1$, seul cas auquel la construction de la figure 35 ne s'applique pas, nous avons recours à la construction de la figure 34, lemme 5.

Le lemme est ainsi démontré.

THEOREME 5

L'opération G est fonctionnelle.

En effet, en vertu du lemme 6, on peut engendrer à partir du combinateur $G_{c,1}$ une structure à une entrée x et une sortie z telle que

$$z = (x+1 \bmod m)$$

Soit S une telle structure (fig. 36) :



Fig. 36

Considérons maintenant la structure de la figure 37 :

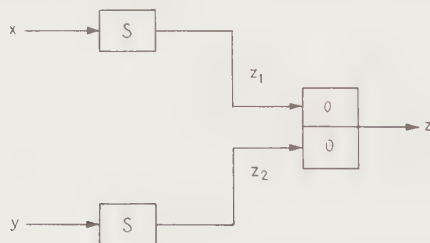


Fig. 37

La sortie z du combinateur $G_{0,0}$ est donnée par ce qui suit

pour $x = y$ $z_1 = z_2 = (x+1 \bmod m)$ donc $z = x+1 \bmod m$

et pour $x \neq y$ $z_1 \neq z_2$ donc $z = 0$

Cette structure est donc équivalente à un combinateur réalisant la fonction de Webb.

L'opération G est donc fonctionnelle, puisqu'elle engendre la fonction de Webb qui est fonctionnelle.

CAS PARTICULIERS

Dans le cas particulier de $m = 2$, il n'est possible de définir qu'un seul cyclage

$$t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

et par conséquent deux fonctions G :

$$G_{01} \qquad \text{et} \qquad G_{11}$$

La première est la fonction de "Peirce" et la deuxième la fonction de Sheffer.

Pour $m = 3$, on définit 6 fonctions distinctes (Il existe en tout 3774 fonctions de Sheffer, dont 90 commutatives).

De façon générale, on définit $m!$ opérations G dans l'ensemble $E = \{0, 1, 2, \dots, m-1\}$.

REMARQUES

a) Nous terminons ce chapitre par une démonstration simple du théorème, dans le cas où le cyclage est une permutation circulaire de r rangs, r étant premier à m .

Considérons en effet la fonction

$$\begin{aligned} P(x, y) &= x + r \pmod{m} && \text{pour } x = y \\ &= c && \text{pour } x \neq y \end{aligned}$$

La construction de la figure 4 (lemme 3) donne, à la sortie

$$\begin{aligned} z &= x + (q+k)r && \text{si } x = y \\ \text{et } z &= c + kr && \text{si } x \neq y \end{aligned}$$

d'où les deux congruences simultanées

$$(q+k)r \equiv 1 \pmod{m} \tag{105}$$

$$\text{et } c + kr \equiv 0 \pmod{m} \tag{106}$$

Pour c et r quelconques, les congruences 105 et 106 ont une solution et n'en ont qu'une si et seulement si $(r, m) = 1$.

Au système des deux congruences correspond donc un couple (q, k) et un seul, pour tout couple (c, r) . La fonction P engendre la fonction de Webb, elle est donc fonctionnelle.

b) La généralisation G aurait pu être établie directement en démontrant tout simplement que cette fonction est isomorphe à la fonction W . Toutefois, nous avons préféré démontrer que G est fonctionnelle en ayant recours à des constructions susceptibles d'illustrer le mode d'assemblage des structures de commutation.

CHAPITRE VII

GÉNÉRALISATION DES FONCTIONS DE POST

Soit $R = a_0, a_1 \dots a_{m-1}$ une permutation quelconque des éléments de E .

Nous définissons dans E l'opération suivante :

$$\begin{aligned} a_i \otimes_R a_j &= a_i & \text{si } i \leq j \\ &= a_j & \text{si } i > j \end{aligned}$$

et soit p_R la substitution

$$p_R(a_i) = a_{i+1} \pmod m \quad \text{pour tout } i \in E.$$

Post a démontré que l'opération $\otimes_R$ et le cyclage p_R constituent un ensemble fonctionnel, quelle que soit la permutation R .

Nous généraliserons ce résultat en montrant qu'il existe d'autres cyclages formant avec l'opération $\otimes_R$ un ensemble fonctionnel.

Pour simplifier l'écriture, nous raisonnerons dans ce qui suit sur les indices des éléments $a_0, a_1 \dots a_{m-1}$ et nous conviendrons que

$$\begin{aligned} j + i &= i + j = i & \text{si } i \leq j \\ &= j & \text{si } i > j \end{aligned}$$

(Cette opération est commutative et associative).

$$\text{et } p(i) = i + 1 \pmod m \quad \text{pour tout } i \in E$$

DÉFINITION

Nous désignons par $H_{q,r,s}(x)$ la fonction de $x \in E$ telle que

$$\begin{aligned} H_{q,r,s}(x) &= r & \text{pour } x = s \\ &= q & \text{pour } x \neq s \quad \text{avec } q, r, s \in E \end{aligned}$$

LEMME 7

L'opération $+$ et un cyclage quelconque engendrent les fonctions $H_{0,1,s}(x)$ pour toutes les valeurs $s \in E$.

En effet, soit σ un cyclage défini dans l'ensemble E , et s un élément de celui-ci.

Il y a un élément j de E et un seul qui satisfasse

$$s^j = 0 \quad \text{c'est-à-dire} \quad \delta_{s0} = j$$

(avec bien entendu $s^j = \sigma^j(s)$).

Désignons par $\overline{j}$ l'ensemble complémentaire de j par rapport à E . C'est-à-dire $\overline{j} = E - \{j\}$.

s est le seul élément de E tel que

$$s^i \neq 0 \quad \text{pour toutes les valeurs de } i \in \overline{j}$$

et il y a une valeur et une seule de $i \in \overline{j}$ telle que

$$s^i = 1.$$

Si nous écrivons maintenant

$$y = \begin{array}{|c|c|} \hline & \\ \hline & \\ \hline \end{array} x^i$$

$i \in \overline{j}$

le symbole $\begin{array}{|c|c|} \hline & \\ \hline & \\ \hline \end{array}$ représentant l'opération $+$ répétée, nous avons :

Pour $x \neq s$, il y a une valeur (et une seule) de $i \in \overline{j}$ pour laquelle $x^i = 0$. Nous avons donc $y = 0$.

Pour $x = s$, il n'y a aucune valeur de i pour laquelle $x^i = 0$, et il y a une valeur (et une seule) de $i \in \overline{j}$ pour laquelle $x^i = 1$. Nous avons donc $y = 1$.

Ce qui nous donne :

$$y = \begin{array}{|c|c|} \hline & \\ \hline & \\ \hline \end{array} x^i = H_{0,1,s}(x) \quad (107)$$

$i \in \overline{j}$

et, en tenant compte de ce que

$$s^j = 0, \quad \text{c'est-à-dire} \quad 0^{-j} = s,$$

nous pouvons écrire

$$\begin{array}{|c|c|} \hline & \\ \hline & \\ \hline \end{array} x^i = H_{0,1,0^{-j}}(x) \quad (108)$$

$i \in \overline{j}$

ou encore

$$H_{0,1,s}(x) = \begin{array}{|c|c|} \hline & \\ \hline & \\ \hline \end{array} x^i$$

$i \in \{\delta_{s0}\}$

DÉFINITIONS

Considérons l'ensemble E^2 des couples $[a,b]$ d'éléments de E . Un couple est dit "vecteur", et désigné par $\langle ab \rangle$.

Nous définissons dans l'ensemble des vecteurs l'ensemble R des vecteurs $\langle ab \rangle$ satisfaisant $\delta_{a,b} \equiv t \pmod{m}$.

La relation ci-dessus définit une classe que nous appelons Réseau de raison t , ou Réseau (t) .

L'ensemble E^2 se partitionne par conséquent en m réseaux, de raisons $0, 1, \dots, m-1$.

Un réseau (t) est une classe cyclique, et peut être engendré (par cyclage), à partir d'un élément quelconque du réseau.

En effet, convenons que :

$$\sigma(\langle ab \rangle) = \langle \sigma(a) \sigma(b) \rangle$$

c'est-à-dire que le vecteur obtenu par cyclage du vecteur $\langle ab \rangle$ est le vecteur dont les éléments sont, dans l'ordre, le cyclage de a et le cyclage de b .

Soient maintenant $\langle ab \rangle$ et $\langle cd \rangle$ deux vecteurs appartenant à un même réseau (t) , c'est-à-dire

$$\delta_{ab} \equiv \delta_{cd} \equiv t \pmod{m}$$

Quels que soient a et c il existe toujours un i et un seul tel que

$$a^i = c$$

et l'on a

$$d = c^t = a^{i+t} = (a^t)^i = b^i$$

d'où

$$\langle a \ b \rangle^i = \langle c \ d \rangle$$

On en déduit qu'un vecteur quelconque engendre, par cyclage, tous les vecteurs de son réseau, et n'engendre que ceux-ci.

Soient maintenant $\langle ab \rangle$ et $\langle cd \rangle$ deux vecteurs appartenant à un même réseau (t) et $\langle ef \rangle$ un vecteur appartenant à un réseau (ϕ) , avec

$$\phi \neq t \pmod{m}.$$

Nous conviendrons d'écrire

$$\langle ab \rangle + \langle cd \rangle = \langle ef \rangle$$

si $a + c = e$ et $b + d = f$

et nous dirons que les vecteurs $\langle ab \rangle$ et $\langle cd \rangle$ engendrent, par minimum, le vecteur $\langle ef \rangle$.

Nous pouvons alors dire que le vecteur $\langle ab \rangle$ (ou le vecteur $\langle cd \rangle$) engendre, par cyclage et minimum, le vecteur $\langle ef \rangle$.

Or le vecteur $\langle ef \rangle$ engendre, par cyclage, un vecteur quelconque du réseau (ϕ) . Nous pouvons donc dire qu'un vecteur quelconque du réseau t engendre, par cyclage et minimum, le réseau (ϕ) , ou encore que le réseau t engendre, par cyclage et minimum, le réseau (ϕ) .

LEMME 8

a étant un élément quelconque de E, il existe une correspondance biunivoque entre les valeurs de $i \in E$ et les vecteurs

$$\langle a^{it} a^{(i+1)t} \rangle$$

du réseau $R(t)$, si et seulement si t est premier à m .

a) A chaque valeur de i correspond un vecteur et un seul du réseau (t) .

En effet, pour un t donné, chaque i détermine un et un seul produit $i \bmod p$.

b) A chaque vecteur de $R(t)$ correspond une valeur de i et une seule si et seulement si $(t, m) = 1$.

En effet, soit $\langle a^j a^{j+t} \rangle$ un vecteur quelconque de $R(t)$. A chaque valeur de j correspond une et une seule valeur i satisfaisant

$$j \equiv it \pmod{m}$$

si et seulement si $(t, m) = 1$.

Il découle de ce lemme que si $(t, m) = 1$, les vecteurs du réseau (t) peuvent s'écrire :

$$a a^t, a^t a^{2t}, a^{2t} a^{3t}, \dots, a^{it} a^{(i+1)t} \dots a^{(m-1)t} a.$$

LEMME 9

Si $(t, m) = 1$, le réseau t engendre, par cyclage et minimum, tous les vecteurs de l'ensemble E_t^2 .

Ceci revient à dire que le réseau t engendre un réseau ϕ avec ϕ quelconque $\not\equiv t \bmod m$, ou encore qu'avec t donné, il existe pour tout ϕ des éléments a, i, j , et k tels que

$$a^{it} a^{(i+1)t \bmod m} + a^{(j-1)t \bmod m} a^j = a^k a^{k+\phi}$$

avec $it \not\equiv (j-1)t \bmod m$, c'est-à-dire $i \not\equiv j-1$.

Si nous posons :

$$a^{it} = a^k$$

c'est-à-dire $it \equiv k \bmod m$, il vient :

$$a^{it} a^{(i+1)t \bmod m} + a^{(j-1)t \bmod m} a^j = a^{it} a^{it+\phi \bmod m}$$

Le problème se ramène à démontrer que pour tout $\phi \in E$, il existe dans E des éléments a, i et j satisfaisant

$$a^{it} < a^{(j-1)t \bmod m} \quad (109)$$

$$a^{(i+1)t} > a^{jt \bmod m} \quad (110)$$

$$jt \equiv it + \phi \bmod m \quad (111)$$

Considérons la congruence 3. Celle-ci s'écrit

$$(j-i)t \equiv \phi \pmod{m}$$

t étant premier à m , il existe toujours une valeur de $(j-i)$ située entre 0 et $m-1$ qui satisfasse cette congruence.

Posons
$$\phi = j-i-1 \pmod{m}$$

Les conditions 1 et 2 s'écrivent alors

$$a^{it} < a^{(i+\phi)t \pmod{m}}$$

et
$$a^{(i+1)t} > a^{(i+\phi+1)t \pmod{m}}.$$

Or la substitution σ étant un cyclage, et t étant premier à m , la substitution σ^t est aussi un cyclage, et les conditions ci-dessus deviennent, par rapport à σ^t :

$$a^i < a^{i+\phi}$$

et
$$a^{i+1} > a^{i+\phi+1}.$$

Si nous désignons l'élément a^i par x , le théorème est démontré s'il est prouvé qu'à toute valeur $\phi \in E$ correspond au moins un élément $x \in E$ tel que, par rapport à un cyclage (σ^t)

$$x < x^\psi$$

et
$$x^1 > x^{\psi+1}$$

Si ceci n'était pas vérifié, il existerait une valeur de ψ telle que

a) $x > x^\psi$ pour tout $x \in E$

ou b) $x^1 < x^{\psi+1}$ pour tout $x \in E$,

résultats contraires à l'hypothèse d'un ensemble E fini.

Le lemme est donc démontré.

LEMME 10

Si σ est un cyclage défini dans E , tel que $\delta_{01} = t$, avec $(t, m) = 1$, l'opération $+$ et le cyclage σ engendrent les fonctions $H_{q,r,s}(x)$ pour toutes les valeurs q, r et $s \in E$.

En effet, dénotons par $H_{q,r,s}^1(x)$ la fonction $\sigma[H_{q,r,s}(x)]$, et de façon générale, par $H_{q,r,s}^n(x)$ la fonction $\sigma^n[H_{q,r,s}(x)]$.

Il découle immédiatement de la définition de la fonction $H_{q,r,s}$ que :

$$H_{q,r,s}^n(x) = H_{q^n,r^n,s}(x).$$

Par ailleurs, on vérifie aisément que :

$$H_{a,b,s}(x) + H_{c,d,s}(x) = H_{a+c,b+d,s}(x).$$

On en déduit que si un vecteur $\langle ab \rangle$ engendre par minimum et cyclage un vecteur $\langle cd \rangle$, il est possible de concevoir un assemblage grâce auquel la fonction $H_{a,b,s}$ engendre la fonction $H_{c,d,s}$ de x , faisant intervenir seules les opérations $+$ et cyclage.

Or nous avons vu au lemme 7 que ces opérations engendrent les fonctions $H_{0,1,s}$ pour toutes les valeurs de s .

Si $\delta_{01} = t$, on en déduit que le vecteur $\langle 0 \ 1 \rangle$ engendre par cyclage et minimum un vecteur $\langle q \ r \rangle$ quelconque, et le lemme est démontré.

THEOREME 6

Une condition suffisante pour que l'opération $+$ et un cyclage σ constituent un ensemble fonctionnel est que la distance δ_{01} (par rapport à σ) soit première à m .

En effet, nous avons vu au lemme 10 qu'un cyclage satisfaisant cette condition, pouvait engendrer avec l'opération $+$ les fonctions $H_{q,r,s}$ pour toutes les valeurs q, r et $s \in E$, donc en particulier, les fonctions

$$H_{m-1, (s+1 \bmod m), s} (x) \text{ pour toutes les valeurs de } s \in E.$$

Considérons maintenant la fonction

$$p(x) = \sum_{s \in E} H_{m-1, (s+1 \bmod m), s} (x).$$

Nous avons, pour $x = i$

$$\begin{aligned} p(i) &= \sum_{s \in \{\bar{i}\}} H_{m-1, s+1 \bmod m, s} (i) + H_{m-1, i+1 \bmod m, i} (i) \\ &= \sum_{s \in \{\bar{i}\}} m-1 + (i+1) \bmod m \\ &= (i+1) \bmod m \text{ pour toutes les valeurs de } i \in E. \end{aligned}$$

$p(x)$ n'est autre que le cyclage de Post. Or celui-ci constitue un ensemble fonctionnel avec l'opération $+$.

L'ensemble $\{+ \text{ et } \sigma(x)\}$ engendre l'ensemble $\{+ \text{ et } p(i)\}$ Le premier est donc fonctionnel.

Pour clore ce chapitre, remarquons que la condition $(\delta_{01,m}) = 1$ n'est pas nécessaire. Nous n'aborderons pas ici les cas où elle ne se vérifie pas et qui correspondent quand même à des ensembles fonctionnels. Une étude générale des conditions nécessaires et suffisantes pourrait présenter un grand intérêt.

RÉFÉRENCES BIBLIOGRAPHIQUES

- [1] a) D.A. HUFFMAN - "The design of Sequential Relay Circuits".
Journal of the Franklin Inst., Vol. 257, 1954 (USA)
- b) G.H. MEALY - "A Method for Synthesizing Sequential Circuits".
Bell System Technical Journal, Sept. 1955, Vol. 34, n° 5 (USA)

- c) E.F. MOORE - "Gedanken-Experiments on Sequential Machines". Automata Studies. Edité par Shannon et Mc Carthy. Princeton University Press, 1956 (USA)
- d) S.C. KLEENE - "Representation of Events in Nerve Nets and Finite Automata". Automata studies (même référence que 1.c)
- e) I.M. COPI, C.C. ELGOT, J.B. WRIGHT - "Realization of Events by Logical Nets". Proceedings of the Association for Computing Machinery, 1958 (U.S.A.)
- f) A.W. BURKS et J.B. WRIGHT - "Theory of Logical Nets". Proceedings of the IRE, 41 (1953) (USA)
- [2] a) E.L. POST - "Introduction to a general Theory of Elementary Propositions". American Journal of Mathematics, Vol. 43 (1921) (USA).
- b) J.B. ROSSER et A.R. TURQUETTE - "Axiom Schemes for M-valued Propositional Calculi".
- [3] G. BOOLE - "An Investigation of the laws of Thought". Dover Publications Inc. (USA)
- [4] E.L. POST (même référence que 2.a)
- [5] H.M. SHEFFER - "A set of five independent postulates for Boolean Algebra". Trans. amer. Math. Soc., 14 (1953) (USA)
- [6] J.D. SWIFT - "Algebraic Properties of n-valued propositional Calculi". Amer. Math. Monthly, vol. 59 (1952) (USA)
- [7] N.M. MARTIN - "The Sheffer Functions of 3-valued Logic". Journal of Symbolic Logic, Vol. 19, n° 1 (1954) (USA)
- [8] NAKAZIMA et HANZAWA - Journal de l'Inst. des Ing. de Comm-Elect. du Japon, n° 165 (Déc. 1936), et 167 (Fév. 1937).
- [9] C.E. SHANNON - "A symbolic Analysis of Relay and Switching Circuits". Elect. Eng. Trans. Suppl., n° 57 (1938)
- [10] H. FREUDENTHAL - "Logique Mathématique appliquée". Monographies réunies par Mme P. FEVRIER, Gauthier-Villars, 1958.
- [11] E. ZYLINSKY - Fundamenta Mathematica, vol. 7 (1925).
- [12] S. PICCARD - "Sur les fonctions définies dans les ensembles finis quelconques". Fund. Mathematica, vol. 24 (1935)
- [13] N.M. MARTIN (même référence que 7)
- [14] J. SŁUPECKI - "Kryterium pelnosci wielowartosciowych systemow logiki zdan". Comptes rendus des séances de la Soc. des Sciences et des Lettres de Varsovie. Classe III, vol. 32 (1939)
- [15] D.L. WEBB - "Generation of any N-valued Logic by one Binary Operation". Proc. Nat. Acad. of Science (USA), vol. 21 (Mai 1935).
- [16] C.Y. LEE et W.H. CHEN - "Several-valued Combinational Switching Circuits". Transactions Paper of the AIEE, n° 56-162 (1956).

- [17] a) J. VILLE - "Eléments de l'Algèbre de Boole" Publications de l'Institut de Statistiques de l'Université de Paris. Vol. 4, fasc. 2 et 3 (1955).
- b) R. SERRELL - "Elements of Boolean Algebra for the Study of information Handling Systems". Proceedings of the IRE, Oct. 1953 (USA).
- [18] J.W. GLAISHER - "On the Residue of a binomial theorem Coefficient with respect to a prime modulus". Quart. Journ. Math., 30 (1899)
- [19] J. ŁUKASIEWICZ et A. TARSKI - "Untersuchungen über den Aussagenkalkül". Comptes rendus des séances de la Société des Sciences et des Lettres de Varsovie. Classe III, vol. 23 (1930)
- [20] J.B. ROSSER et A.R. TURQUETTE - "Many-Valued Logics". North Holland Publishing Co (1952)
- [21] J. ŚŁUPECKI - "Der volle dreiwertige Aussagenkalkül". Comptes rendus des séances de la Société des Sciences et Lettres de Varsovie. Classe III, vol. 29 (1936)
- [22] T. EVANS et P.B. SCHWARTZ - "On Slupecki T-Functions". The Journal of Logic Symbolic Logic. Vol. 23, n° 3, Sept. 1958.
- [23] M. DANLOUX-DUMESNILS - "Les systèmes de numération et les calculatrices automatiques". Mesures, n° 256, Sept. 1958.
- [24] a) TURING, A.M. - "On Computable Numbers" Proc. of the London Math. Soc. 2-42 (1936).
- b) PORTE, J. - "Une simplification de la théorie de Turing" Actes du 1er Congrès International de Cybernétique. Namur (Belgique) 1956
- [25] VON NEUMANN J. - "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components" Automata Studies (même référence que 1.c).

TABLE DES MATIÈRES

INTRODUCTION	1
Chapitre premier - DÉFINITIONS	
Elément combinatoire	5
Combinateur	6
Structure de commutation	6
Chapitre II - FONCTION DE TRANSFERT	
Caractérisation arithmétique des fonctions de transfert	11
Analyse et synthèse des structures combinatoires	13
Ensembles complets ou fonctionnels	14
Ensemble semi-fonctionnel	15
Chapitre III - RAPPEL DE QUELQUES RÉSULTATS CONCERNANT LES ENSEMBLES FONCTIONNELS	
Chapitre IV - L'ENSEMBLE SEMI-FONCTIONNEL, SOMME, PRODUIT, IDENTITÉ	
La somme	21
Le produit	22
Fonction Identité	24
Propriétés remarquables de la somme	24
Propriétés remarquables du produit	24
Autre propriété remarquable de la somme et du produit	33

Chapitre V - POLYNOMES MODULO P

Première partie	35
Cas d'une variable unique	39
Cas de n variables	42
Deuxième partie	51

Chapitre VI - GÉNÉRALISATION DE LA FONCTION DE WEBB

Cyclage	59
La fonction G	61
Cas particuliers	67

Chapitre VII - GÉNÉRALISATION DES FONCTIONS DE POST

RÉFÉRENCES BIBLIOGRAPHIQUES	74
---------------------------------------	----

DEUXIÈME THÈSE.

PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Théorie et application de l'équation intégrale de Wiener-Hopf.

Vu et approuvé :

Paris, le 14 mai 1959.

LE DOYEN DE LA FACULTÉ DES SCIENCES,

J. PÉRÈS.

Vu et permis d'imprimer :

LE RECTEUR DE L'ACADÉMIE DE PARIS,

Jean SARRAILH

PARIS. — IMPRIMERIE GAUTHIER-VILLARS

Quai des Grands-Augustins, 55.

156221-59

Dépôt légal, Imprimeur, 1959, n° 1372.

Imprimé en France.

PARIS. — IMPRIMERIE GAUTHIER-VILLARS

Quai des Grands-Augustins, 55.

156221-59

Dépôt légal, Imprimeur, 1959, n° 1372.

Imprimé en France.